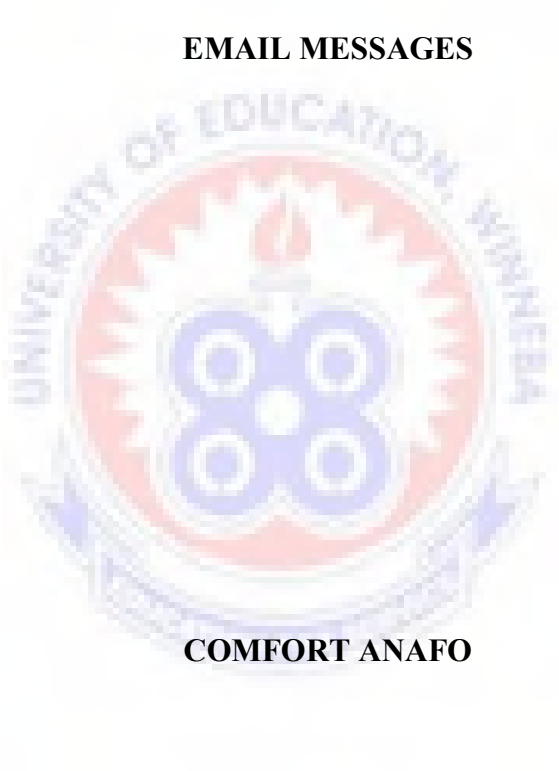
UNIVERSITY OF EDUCATION, WINNEBA

THE LANGUAGE OF DECEPTION: TRANSITIVITY ANALYSIS OF SCAM EMAIL MESSAGES



COMFORT ANAFO

2017

UNIVERSITY OF EDUCATION, WINNEBA

THE LANGUAGE OF DECEPTION: TRANSITIVITY ANALYSIS OF SCAM EMAIL MESSAGES

COMFORT ANAFO

(8150060016)

THESIS SUBMITTED TO THE DEPARTMENT OF ENGLISH EDUCATION OF THE FACULTY OF FOREIGN LANGUAGES EDUCATION AND COMMUNICATION, UNIVERSITY OF EDUCATION, WINNEBA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR AWARD OF MASTER OF PHILOSOPHY IN ENGLISH DEGREE.

SEPTEMBER, 2017

DECLARATION

STUDENT'S DECLARATION

I, COMFORT ANAFO, declare that this Thesis, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my own original work, and it has not been submitted, either in part or whole, for another degree elsewhere.

SIGNATURE: ……

DATE: ……

SUPERVISOR'S DECLARATION

I hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of Thesis as laid down by the University of Education, Winneba.

NAME OF SUPERVISOR: Dr. Richmond Sadick Ngula

SIGNATURE: ……

DATE: ……

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor, Dr. R. S. Ngula for the encouragement and support he gave me; not forgetting his insightful comments on my thesis. I appreciate his patience and guidance during this study.

I would also like to thank all the lecturers in the Department of English Education, University of Education for providing a great environment for studying.

My special thanks go to my father and friend, Dr. Samuel A. Atintono, for being a pillar to me.

I thank Dr. Isaac Mwinlaaru and Kenneth Bodua-Mango for the encouragement and guidance they gave me throughout this study.

Thanks to all my friends and colleagues for their support, patience, and understanding when I did not have time to spend with them.

Finally, I want to thank my family especially, Dr. Annabel Ankrah at Ridge hospital, Accra, for being optimistic and encouraging me throughout this study.

DEDICATION

In memory of my beloved brother,

JAMES BABA AWUNI

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

SFL: Systemic Functional Linguistic

DA: Discourse Analysis

CMC: Computer-Mediated Communication

MUDS: Multi-User Dimensions

CBCA: Criteria-Based Content Analysis

RM: Reality Monitoring

LIWC: Linquistic Inquiry and Word Count

SCAN: Scientific Content Analysis

VI: Verbal Immediacy

IDT: Interpersonal Deception Theory

STX: Scam Text Message

CL: Clause

MD&A: Management Discussion and Analysis Sections

ABSTRACT

The increasing use of the internet has also increased the chances of receiving scam emails. Several linguistics approaches have been used by researchers to conduct several studies on deception. Even though these approaches have helped to detect deception, they focus on aspects of the texts as opposed to a holistic analysis of the functional orientation of the texts. This study examines how deception is construed through linguistic choices, by first breaking up email texts into clauses, and then following up with a detailed clause-by-clause analysis. The focus of the study is on the transitivity choices used by email scammers to construe fraud in an attempt to manage information in order to manipulate email recipients. The data consist of forty scam email messages solicited from various recipients and also downloaded from a website. The study made several findings: first, transitivity patterns of the material processes in scam email messages show that the scammers variously position themselves as negotiable, vulnerable and generous; second, transitivity patterns associated with the relational processes reveal the identity of the scammers as credible and respectable persons in society; third, the identified mental clauses demonstrate that scammers feign commitment and dedication in the scam email messages; fourth, the patterns show that the Sayers in verbal processes are usually thanking the recipients, blessing the recipients, and seeking for assistance from the recipients. The behavioural process was used to urge recipients to respond to the scam emails while the existential process was used to motivate the recipients to reply to the emails. The study finally concludes that various linguistic strategies were deployed by the scammers to manipulate target recipients.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

The aim of this study is to investigate the linguistic construction of deception in scam email messages. The present chapter provides a general introduction to the study. First, it discusses the background of the study and the motivation for which it was conducted. This is followed by the statement of the problem, the purpose of the study and the research questions. In addition, the chapter discusses the significance and delimitation of the study and concludes with an outline of the thesis.

1.1 Background to the Study

The study is situated within the scholarship on computer-mediated communication (Section 1.1.1), in general, and email communication (Section 1.1.2), in particular.

1.1.1 Computer-Mediated Communication

Computer-mediated communication is the predominant means of communication in recent times. CMC is the broad term used to refer to all communication via the computer. Scholars have defined CMC from different perspectives. December (1997) gives an elaborate definition of computer-mediated communication as "the process of human communication via computers, involving people, situated in contexts, engaging in a process to shape media for a variety of purposes". This definition points out the important participants needed in CMC, namely, the 'computer', 'people', and 'contexts'. Another definition is given by Romiszowski and Mason (1996) as

"communication between different parties separated in space and/or time, mediated by interconnected computers." There is a common element in the definition of Computer-Mediated Communication given by these two scholars, that is, 'computers'. The primary means of Computer-Mediated Communication (CMC) is through (the of) computer. Romiszowski and Mason further explain that the computer is used in place of printed paper which was the main means of sending messages before Computer-Mediated Communication.

Computer-Mediated Communication comes in different forms, such as text, video or audio. The textual form of communication is the primary focal point of this study. The text allows various configurations of communication, including email, discussion lists, web forums, chat, Multi-User Dimensions (MUDs), instant messaging, text messaging, weblogs (blogs) and microblogs (Herring and Storerger, 2014). In the textual form of communication, there is a lack of facial expression or voice, unlike the videos where the faces of the people involved in the discussions are seen or the audio where the voice of the recipient is heard. The main means of communication in the textual computer-mediated communication is the text. In this study, my attention is limited to the text-based CMC in scam emails. Video and audio scams are excluded from this study. The study also excludes scam emails presented in a form other than text. The reason for focusing on the text is to examine the linguistic items in scam emails.

1.1.2 Email Communication

The internet has changed the communication pattern of people, both locally and globally over the past twenty years (Baron, 2003). It has become an important medium by which people send information, advertise all kinds of things and even do

transactions. Hancock, Ockleford, and Windridge (2007) indicate that although this modern communication technology has brought a lot of merit, like faster and cheaper means of sending information, it has also increased the rate of deception online. The ever-increasing use of the internet for transferring information has indeed also increased the chances of online deception, thereby making it difficult to manually filter and screen such messages (Zhou, Burgoon, Twitchell, Qin, and Nunamaker 2004). There are many concerns about online deception. According to Toma and Hancock (2012), these concerns originate from the fact that, in online interaction, there is a lack of physical appearance, which increases the chances of the occurrence of various kinds of deception.

One common mode of online deception is the use of a scam email message, a fraud email that potentially extorts money and property. Spoofing, phishing, lottery scam are types of email fraud. The sender usually fakes his or her identity in order to carry out such acts to either steal money or perform a criminal act. Identity fraud involves the stealing of financial or other private information (identity theft) or using totally invented information to make purchases or gain access to financial accounts (Hinde, 2005). There are several definitions of deception by scholars from different perspectives. Deception is defined in the context of this thesis as the "deliberate attempt, whether successful or not, to conceal, fabricate and manipulate either factual or emotional information by verbal or non-verbal means in order to create or maintain in others a belief the communicator himself considers as false" (Masip, Garrido, & Herrero, 2004).

Salvetti, Lowe, and Martin (2016) distinguish 'deception' from 'lying', noting that deception is intentionally made up to cause another person to believe in something which is false while lying involves making a false statement to another person with

the intention that the person believes that statement to be true. However, it cannot be said that deceptions and lies are totally separable since they are both false stories which the sender conceals as true. Deception, however, involves manipulation in order to achieve an end.

1.1.3 Motivation for the Study

This study was motivated mainly by the growth of online deception in business, law enforcement, and national security. The main reason for embarking on this study is (based on my observation of) the increasing incidence of online fraud in recent years. Many businessmen and private individuals have been duped millions of cedis by scammers; 'the largest 419 scam on record is a crime that led to the collapse of Banco Noroeste in Sao Paolo, Brazil after Nigerian scam perpetrators siphoned US$242 million from the bank' (Blommaert & Omoniyi 2006PAGE NUMBER).

This study, therefore, explores deception in online scam messages to show how deception is linguistically presented in such texts. The study thus limits itself to the linguistic cues of deception based on a corpus compiled from the internet.

Although several studies have been done on the language of deception (Blommaert & Omoniyi, 2006; Hancock, Thom-Santelli, & Ritchie, 2004), people still fall prey to the deceptive work of scammers on the internet daily. It is important to still study the language of deceptive, especially scam emails, and explore the pattern of deceptive language to reveal the hidden meaning of those patterns as well as the linguistic choices scammers employ. These linguistic cues, hopefully, will create more awareness of deception online. The study will also contribute to the scholarship on how language is used to construct deception.

1.2 Statement of the Problem

The growing use of the internet has also increased the chances of receiving scam emails. Scam is now part of the internet and it is very difficult to control since the users cannot determine which emails they want to see in their inbox and which ones they do not want to see. Zhou, Burgoon, Numaker and Twecgell (2004) indicate that several linguistic approaches have been used by researchers to conduct studies on deception.

Toma and Hancock (2012) used the language-based approach in studying deception in online dating platform. Driskell and Neuberger (2014) used Linguistic Inquiry and Word Count Analysis (LIWC) to analyze the language of deception. Carlson, George, Burgoon, Adkins, and White (2004) used the Interpersonal Deception Theory and Channel Expansion Theory to analyze deception in email scam messages. Linguistic Inquiry and Word Count (LIWC) defines words based on a dictionary meaning. Concerning the LIWC, the dictionary does not take into account the context in which a word was produced. This limits the studies that use the LIWC analysis because, certain words are best understood when considered in context. Also, the Interpersonal Deception Theory analysis is based on propositions which is also limited because, words which do not fall within the proposition of the theory will not be considered. Even though these approaches have helped to detect deception, they focus on aspects of the texts as opposed to a holistic analysis of the functional orientation of the text. Thus, our knowledge of deceptive scam emails from a linguistic perspective is still very limited as very few studies exist on this topic. A holistic analysis has the advantage of revealing hidden meanings and how linguistic forms that are unsuspected as strategies of fraud are used by scammers to deceive their victims. This study will examine how deception is construed through linguistic choices, by first

breaking up clause complexes into simple clauses, and then following up with a detailed clause-by-clause analysis. The focus of the study is on the transitivity choices (i.e. verb choices and participant roles involved) used by email scammers to construe fraud in an attempt to manage information in order to manipulate email recipients.

This research thus takes a linguistic approach to studying deception; it examines the function of clauses (transitivity pattern) in fraud email messages and not just grammatical structures alone. In this case, examining the function of the clauses will help detect deception both explicitly and implicitly in terms of the meaning these clauses convey. Following Halliday (cf. Halliday & Matthiessen, 2014), the study takes a functional perspective towards language and primarily assumes that the language of a text reflects the functions the text performs. Thus, since transitivity is the main grammatical system by which experiences and consciousness (or world-view) are transformed into linguistic meaning, a study of fraudulent email messages should reveal how deception is constructed in language.

1.3 Objectives of the Study

As mentioned earlier, the general objective of the study is to investigate what resources of transitivity are used by scammers in the construction of deception and manipulating email recipients. The specific objectives are, first, to examine the process types used in manipulating recipients of scam emails and, second, to examine patterns in the process types, plus participant configuration that scammers deploy and show how they reveal the manipulative purpose of scamming.

1.4 Research questions

The study is guided by the following research questions:

1. What process type(s) is/ are used in scam emails?
2. (a) What transitivity pattern(s) is/ are used in scam email messages to construe fraud?

   (b) How do they reveal the manipulative purpose of scamming?

1.5 Significance of the Study

This study will add to the growing research and studies on scam language and contribute to the understanding of the language of scam emails, focusing specifically on transitivity. The findings of this study will help identify the linguistic choices that scammers use to construe deceptive messages. The study will therefore be significant to research on language and deception, the theoretical relationship between linguistic form and linguistic function and the practical application of linguistic research in forensic contexts for the detection of cues of fraudulent communication.

The value of the study is also highlighted by its contribution to research on Cyber fraud, especially email scam. Although email scam has become an important area of study (cf. Chhabra, 2005; Freiermuth, 2011), studies have not examined how email scammers represent fabricated experience from the functional-semantic point of view adopted in this study. The study analyses scam email messages clause by clause to identify patterns of ideational meaning and how they reveal the manipulative purpose of scamming. This will add a new approach to the study of scam email messages and deepen our understanding of the world of scammers.

Further, Michael Halliday's systemic functional linguistics (SFL), in general, and his transitivity framework, in particular, have been applied to different texts from several

disciplines. Indrayani and Seomantri (2014) applied transitivity to Shakespeare's sonnet, Ignatieva and Rodríguez-Vergara (2015) also applied transitivity to expert and student research articles. The present study extends this body of literature study by exploring transitivity in scam email messages and further explains how the patterns reveal the manipulative purpose of scamming. The findings of this study will contribute to the application of transitivity to the study of language in critical contexts and extends its validity as a tool for applied linguistic analysis.

1.6 Delimitation

Scam is performed through several modes of communication, such as face-to-face, telephone conversation, social media and email messaging. Although it will be interesting to examine the language of scam in all these modes, the present study is limited to scam email messages due to the fact that they are relatively easy to access without intruding upon the privacy of email recipients and within the time limits set for the present study. Scam email messages also provide an opportunity for the close text analysis adopted in the present study.

1.7 Outline of the Study

The study is organised into five chapters. The present chapter has given a general introduction to the study, the statement of the problem, objectives of the study, research questions, significance of the study and delimitations of the study. Chapter two reviews literature relevant to the study, including theoretical and conceptual reviews and the discussion of empirical studies related to the study. Chapter three also deals with the methods and procedures employed in collecting and analysing the data for this study. Chapter four starts with the analysis, interpretation, and discussion of the data in relation to the research questions. Chapter five gives a summary of the

whole study, the research findings and conclusions. It also makes recommendations for further research.

1.8 Summary of the Chapter

This introductory chapter has provided a general background to the study. First, it gives an introduction to the study and the motivation for which it was conducted. This is followed by the statement of the problem, objectives of the study, the research questions, significance and delimitation of the study. It concluded with an outline of the thesis.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter is in two parts. The first part discusses empirical issues related to the study. This includes the definition of terms such as deception, spam, scam and a description of the approaches to the study of deception in linguistics. Empirical studies related to linguistic or discourse analysis of online deception is also discussed in the first part. The relationship between previous studies and the present study on online deception is also discussed in the first part. The second part focuses on theoretical issues: Systemic Functional Linguistics (SFL) and transitivity, which constitute the framework used for this study. The chapter ends with a demonstration on how Systemic Functional Linguistics (SFL) is applied in the study.

2.1 Defining Deception

In today's society, it is common to find people telling lies for various reasons such as to gain properties, to make themselves comfortable, to portray features they do not possess in order to, sometimes, protect themselves from harmful circumstances (DePaulo et al., 2003). It is this act of telling lies for such reasons that is referred to as deception. Different scholars define deception from different perspectives. According to DePaulo et al. (2003), deception is when one makes a conscious and deliberate attempt to manipulate others. Zhou et al. (2004) also define deception as the active transmission of messages and information to create a false conclusion.

The concept of deception has been of interest to many scholars in recent times and, has been studied from various perspectives including computational linguistics, speech and multimodal processing (Pérez-Rosas et al., 2015).

The general consensus is that people lose valuable property, money, houses, among others, and as a result deception detection has become a very important area of study so as to find ways of preventing such loss of property. Scholars using different approaches have studied deception detection. Some of the approaches used in the study of deception detection are reviewed later in the sections below.

2.2 Defining Spam

Until recently, spam was an object of study in forensic research (Chhbra, 2005). It has however gained currency among linguists in the past decade or so. Linguistic studies of spam, for instance, have considered the linguistic cues for identifying spam (Tabron 2016; Tsikerdekis & Zeadally 2014). Even though one major means of online deception is the use of spam messages, there is no consensus as to what exactly constitutes spam. Hershkop and Stolfo (2006) assert that it is very difficult to single out one definition of spam because a mail may not be requested or wanted by a recipient, but can be useful to him later.

Christina, Karpagavalli and Suganya (2010) define spam as any message or posting that a person does not need but has been sent to his/her email. Christina, Karpagavalli and Suganya (2010) note that the habit of sending bulk mail to people's email regularly when they do not want it is spam. Khong (2001), as cited in Cukier, Cody and Nesselroth (2006), defines spam as any email message, which is unsolicited, sent to people or organisation without considering the identity of the recipient. Spam is also defined as "an email the user does not want to receive and has not asked to receive" (Hershkop & Stolfo, 2005b). Cukier, Ngwenyama, and Nesselroth-Woyzbun (2008) also define spam as unwanted emails that users receive. When we look at the definitions of spam given by different scholars as displayed above, there is one common element that runs through all them, that is, the spam message is unsolicited

or unwanted. This means that users do not have a choice in determining whether to receive spam or not. Spam could be sent at any time to an email user account without any prior notice. Email users tend to recognise a spam email message without opening it (Hershkop and Stolfo, 2006). The user determines whether an email is a spam or not based on the physical cover of the email.

There are different types of spam such as blog, link, wireless and phishing spam. Blog spam usually comes in the form of commercial transaction. Link spam places links to other websites or email. Phishing is rather different because it is used to trick the receiver as the sender fakes his identity in order to get access to valuable information about the recipient. Scam is one type of spam email and the focus of this study is on scam. The next section defines scam.

2.3 Defining Scam

Scam email is a particular type of spam used to dupe victims of monies, properties, and other valuables, not to mention the psychological and emotional harm it causes victims. There are various types of scam, such as black money scams, lottery scam, employment scam, rental scam, work-at-home scam, romance scam and publishing scam. Scam email is mostly referred to as 419 scam, advance fee fraud or Nigerian scam letter. It is called Nigerian scam because it is believed to have originated from Nigeria. According to Ottenheimer and Ottenheimer (2006), over 90% of 419 letters claim to be originating from Africa and the scammers themselves claim to be Africans. Isacenkova, Thonnard, Costin, Francillon and Balzarotti (2014) define scam email as a type of online fraud used to dupe victims of their monies and properties with a promise of a huge sum of money in future. The scammers usually request for monies from the victims and promise them bigger returns when the deal is complete. This never happens as the scammers continuously request money from their victims

and never reciprocate. The easy access to the internet has made it possible for scammers to operate easily without any stress (Edwards, Peersman & Rashid, 2017). Once the scammers have access to the internet, they can send bulk scam messages to different email accounts within a short period of time. Scam emails are studied from the discourse perspective in this study.

2.4 Discourse

The term 'discourse' lends itself to several definitions. But a common definition from a linguistic point of view is that discourse analysis involves the linguistic study of the language used in communication (Trapper-Lomax, 2004). In discourse analysis, the main focus of the linguist is on certain factors such as participants involved in the communication, the cultural background of the participants, the setting and the choice of words of the participants. According to Brown and Yule (1983) discourse is the study of language in use. Discourse analysis deals with examining the relationship that exists between language and the context in which it is used (McCarthy, 1991). Discourse has been studied from an ethnomethodological and a functional approach to language. The ethnomethodological approach studies genres such as storytelling and greeting rituals of people in their natural setting, while the functional approach studies the function of language and speech and the theme of such written or spoken text (McCarthy, 1991).

This present study is situated within the broader field of Discourse Analysis (DA) because DA is committed to the analysis of language beyond the text and challenges the analyst to consider other relevant issues outside the text (Galasinski, 2000). This study considers the context of online fraud in interpreting the analysis of scam messages.

2.5 An Overview of Approaches to the Detection of Deception

Several approaches have been used by scholars to study the language of deception. This section provides a general review of some of the approaches used to study deception, namely, the physiological, nonverbal and text-based approaches. The section gives prominence to the text-based approach, which is the main focus of the present study.

2.5.1 Physiological Approach

The physical behaviors of people can help detect deception using specially manufactured tools (Adams, 2002). Among such tools are polygraph and pupillograhy. The polygraph is used to assess changes in blood pressure, respiratory and electrodermal response. The belief is that people's impulses tend to increase when they are lying. The pupilography examines the size of the pupil and the stress in the voices during speech (Stern, Ray, & Quigley, 2001)

The tools and equipment used in the physiological studies cannot be used by an ordinary person. This means that one needs to be trained to use such equipment and tools. For this reason, it will be difficult to use it to measure deception easily, because once there is a mistake in the setup or in the use of the machine, the results will most likely be incorrect.

2.5.2 Nonverbal Approaches

The nonverbal approach to the detection of deception is examined based on bodily movements and the manner in which an individual speaks. Studies within this approach are exemplified by Masip, Garrido and Herrero (2004) and Vrij, Edward, Roberts and Bull (2000).

Masip, Garrido and Herrero (2004) did a study using 39 existing studies which were conducted using the nonverbal approach. Masip, Garrido and Herrero (2004) concluded that the nonverbal approach to detecting deception is not completely inaccurate as some studies portray. However, there are three main reasons why scholars usually see the results as such. It is usually due to an error in the data. First, the participants used in nonverbal studies are lay people and do not have any prior training. Second, they also believe there is a difference in accuracy when detecting truth using verbal and nonverbal approaches and third, they believe there can be some inaccuracy when there is a powerful external influence on the variables used for the study. They then claim that if researchers used nonverbal approach for the detection of deception, valid and accurate results can be drawn from those studies.

Vrij, Edward, Roberts and Bull (2000) posit that observers usually do not give accurate results when they are observing the nonverbal cues than when there is a criterion used to measure deception. Professional or trained individuals are usually used in nonverbal studies and, even with these experts, sometimes there are pitfalls in their observation. This makes the nonverbal approach to the detecting of deception not reliable (Vril, Edward, Roberts & Bull 2000).

The first section has provided a brief general review of other approaches used to study deception such as the physiological and nonverbal and the limitations associated with these approaches. The limitation of these approaches (physiological and nonverbal) cause inadequacies in the results of analyses of deception. The section below then discusses in detail the text-based approach to the study of deception (section 2.5.3).

2.5.3 Text-Based Approach

The text-based or verbal approaches are similar to the non-verbal approaches in the sense that they both have to do with the observation of behaviour. The difference is that the text-based approach is concerned with the observation of linguistic behavior rather than physiological behaviour. These text-based approaches to the detection of deception involve the study of spoken or written discourse. The researcher analyses the language used in the text in order to find out the function that it performs. There are numerous criteria used in the examination of spoken and written discourse. Both oral and written narratives have been studied using the Criteria-Based Content Analysis (CBCA), Reality Monitoring (RM) and investigative Discourse Analysis to identify deception (Rabon, 2003).

In their study Newman et.al.' (2003) reveal that deceptive messages contain less complex expressions and more negative expressionss. They further add that liars can be caught by what they say alone, that is, the verbal content of their stories, without studying their other behaviours. Since this study is text-based, prominence will be given to empirical studies on the text-based approach which is discussed below in (section 2.6) below.

2. 6 Empirical Linguistic Studies of Deception

The second part of this chapter deals with relevant empirical studies in deception detection from a linguistic point of view in order to establish the relationship between previous studies and the current study. The review broadly consists of studies on scam emails (Section 2.6.1) and studies on other text types that provide some conceptual background to the present study (Section 2.6.2).

2.6.1 Studies on Scam Emails

Linguistic studies on scam emails can be grouped into two main areas, namely studies on general discourse strategies used by scammers to manipulate scam email recipients (Section 2.6.1.1) and those on the rhetorical structure of scam emails (Section 2.6.1.2).

2.6.2 Discourse Strategies in Scam Emails

The first study to consider is by Jiménez and Belli (2013). They examine communicative strategies used by scammers in order to generate some emotional feelings in the recipient. The study demonstrates how spam emails are used to invoke emotions of the recipients. The main focus of the study is on emotional items in spam which raise the emotions of the recipients. The findings show that female writers produce more emotional and affectionate words than their male counterparts in spam emails. Male-sender spam emails were mostly concerned with business or financial transaction. The findings also show that there are instances in which the scam emails generate fear. The scam emails which generate fear and panic were mostly associated with death. The deaths portrayed in scam emails are associated with three main groups of people in the emails. They are; the person sending the message is on a death bed, the death of a relative and the death of a client. The messages usually give the impression that there is a huge sum of money the dead person left behind, which the sender wants to gain through the help of the recipient.

The findings conclude that scam emails have the same features as fairytales, because they contain a lot of imaginary stories which are a common characteristic of fairytales. Spam emails usually contain narratives about people who need help urgently and the recipient is needed to offer such help. The narratives are usually

centered on a sick person who needs help to fulfill his last wish or a dead client who had no next of kin and the writer wants the recipient to act as next of kin. These kinds of stories are usually portrayed in fairytales.

Blommaert and Omoniyi (2006) examine three competencies that authors of scam email messages must possess in order to make a meaningful impact using such messages. The three competencies analysed are technological competence, cultural competence and linguistic competence. Fifty-two scam messages sent to the inboxes of the researchers were analysed for this study. The researchers identified two distinct constructing genres in the scam email. The emails which appeared in the form of lottery messages contained technical and procedural registers. Registers of personal involvement, rapport and faith were identified in the messages which appeared in the form of narratives of experience and trust. It was also established from this research that, scammers do not just write anything but they construct a specific type of text that is meant to present good and reasonable meanings. Even though the writers had a good command of their technological abilities, they, however possessed poor literacy skills needed to make the messages standard. The narratives contained a lot of inconsistent punctuation, use of informal style in formal style, which proves that the literacy skills of the writers were very poor. The writers lacked the ability to produce the standard variety of English. Therefore, they usually cover up their disability by writing short messages, so as to avoid being exposed by their bad grammar. The basic rules and regulations of the English language were also violated in their messages. Linguistic competence was poorly displayed by the writers of scam emails. This study concludes that writers of scam email possess good technological competence, cultural competence, but do not have the appropriate linguistic competence required to write Standard English letters. This study contributes to our knowledge of the abilities

possessed by scam writers, which are, technological abilities and cultural awareness. The study also demonstrated that writers of scam emails lack linguistic abilities and, for that matter, make a lot of linguistic errors in composing scam emails.

The main concentration of this study is whether the scammers possess the technological, cultural and linguistic abilities required to write Standard English scam messages. The study does not analyse the linguistic elements in the emails, but rather, the study is more interested in whether the writers possess the linguistic ability to succeed in composing scam emails. The study could have yield different results if the linguistics elements were considered alone as a strategy writers use to compose scam emails.

Behnam, Azabdaftari, and Hosseini (2011) examine spam to uncover persuasive strategies that spammers employ in their emails. The study focuses on three main categories. These categories are personalization, presupposition and lexical choices. The findings reveal that personalization can be used as a persuasive strategy to pretend that the audience is the only one with whom the writer is communicating.

Rich (2015) analyses over half a million scam email through automated content analysis. The study analyses the pattern of scam email and perception of similarly worded letters through an experimental web design. Suggestions are given to the scammers after the analysis and three of the suggestions are given below;

1. “appeals to trust and the size of the award have only minimal influence at best on public perceptions, while exposure to such offers in the past greatly reduces one’s perceptions’’.

2. "rather than attempt to lure dupes through confidence building language or larger monetary offers, scammers should simply attempt to find those who have not received such offers before''.
3. "trust building rhetoric potentially distracts the reader away from the amount offered, but the causal mechanism here remains unclear''.

Holt and Graves (2007) explore content and methodologies employed in fraudulent messages. The main focus of their study is on the structure and content of fraudulent messages. Four hundred and twelve emails were collected from two state universities email accounts for this study. The researchers notice that the subject lines of scam emails are made to entice the recipients to respond. For instance, the researchers observe that some of the scam emails are created with urgent subject lines while others have a friendly subject line. These are all strategies employed by senders of the messages to get the recipients to read such messages. Also, it is noticed that in the scam emails, senders usually give their gender as male, that is, they mostly portray themselves as male.

The content of these fraudulent messages also have many explicit details about the senders and their purposes for sending such messages. The content of the messages also have inappropriate capitalization, spelling errors and grammatical errors, as well. The senders also attempt to convince the recipients that the transaction is risk-free. The senders are aware of the risk involved in carrying out such a transaction online so they try to convince the recipients in order to win their trust. Religious comments and greetings were also observed in the scam emails especially those messages relating to charity.

This study has provided some basic knowledge about the fact that fraud emails do not usually contain the appropriate linguistic items but rather errors are consistent in fraud emails. The procedures employed by fraudsters to carry out their deceptive intentions are also planned by the writers and the fraudsters intentionally always withhold vital details in the emails they send to recipients.

Tan and Davi (2017) study a deconstruction of a 'romance scammer's online persona', identifying his personal attributes and showing how these attributes establish a sense of credibility. The data comprise 21 emails from Royal Malaysian Police. Six of the emails belong to the victim and fifteen belong to the scammer. The findings of the study reveal that the scammer deliberately presents himself as a person with good character.

Moreover, the text shows thematic relations. The thematic relations portray the intentions of the scammer to hide his true self and create an imaginary figure. The scammer creates an impression which portrays him as a person from a well-educated and wealthy family. The scammer also identifies himself with a rich country such as London or the United States of America. The scammer then projects himself as someone with a very good career who has a sustainable income and a great deal of wealth.

Also, the scammer makes a conscious effort to develop a strong emotional bond with his target by expressing keen attraction for the target. The emotional bond is meant to win the heart of the target. This will make it easier for the scammer to carry out his deception.

This study has revealed that scammers hide their true identity and rather portray themselves as someone they are not. They also use words which are more emotional and affectionate to win their target's trust.

Shafqat, Malik, and Kim (2016) explore the linguistic cues that differentiate scam campaigns from non-scam. The data was collected from *Kickstarter*, a crowd funding site. Three interesting findings were revealed after the analysis.

1. Scammers deliberately try to deceive people by intentionally providing less information and writing more carefully and less being informal.
2. Scammers make less typographical errors than the non-scammers.
3. Expressiveness in the language of scammers is low, due to over-control and less conviction about what is being said.

These findings demonstrate that scammers make conscious effort to hide vital details from their recipients. Also, since the main intention of scammers is to convince their target in believing their deceptive stories, they carefully choose their words so as to win the trust and confidence of the recipients.

Hiß (2015) examines linguistics strategies used by scammers to transmit a sense of identity and authenticity, establish a mutual relationship between sender and receiver and involve the recipient personally. The main aim of this study is to find out how the text is used to construct identities and create personal relationships with recipients. The data for this study consist of hundred scam emails. The data used for the study contains different stories in a narrative form.

The study reveals that scammers use the first person narrative to narrate private identities while, the third person or second person narrative is used to narrate institutional identities. The third person gives the senders an identity of belonging to a

profession, or a social class. The scammers display knowledge of stylistics in the scam emails to enhance the identities they impose on themselves. The mismatch between indexicality and claimed identity exposes the scammer's insufficient control of grammar and genre layout.

Edwards, Peersman and Rashid (2017) examine the persuasive tactics employed by scammers once their victims respond to a scam message. The first part of the study presents an approach which can automatically distinguish advance fee fraud related emails from regular professional and personal emails. The researchers also examine the different communication stages employed by scammers when scamming in online conversations. The semantic markers and scam baiting conversations were also analysed in the study. Scam baiting conversation happens when the victims decide to waste the time of a scammer after they notice the intentions of the scammers. The data was collected from public transcripts posted by members of the 419 Eater Scam Baiting Community Archives and Members Forum. The data was collected from a site called *ERON*. A total of fifty-seven (57) samples were employed for this study.

The study shows that scammers use various persuasive techniques to wooe their victims. The scammers employ a particular persuasive technique at different stages of the conversation based on the communicative function of that stage. The researchers identified that solicitation is the first semantic element employed by scammers. The solicitation is the beginning stage, where scammers try to win the trust of their victims. In the solicitation phase, scammers pose as a person of authority and a trustworthy person. The scammers also promise the victims reward and demand an urgent response from the recipients. The second linguistic item they identify is formal extraction. Formal extraction is the stage where the scammers begin to extort money from their victims after they have won their trust. The scammers usually give money

transfer numbers for the victims to pass money through. The scammers also refer the victims to legal issues and the financial constraints they are facing. The third semantic item identified was an irritation. The scammers employ this strategy when they notice that the scammers are not yielding to their demand. The scammers then employ negative words on their victims. They also remind the victims of the secret agreement they had earlier and vow to terminate the arrangement. The scammers use this strategy to put pressure on their victims to respond to their deceptive desires. The scammers finally employ personal appeal when all effort to get their victims to respond fails. They portray themselves as people one can trust.

This study has demonstrated that scammers plan their deceptive emails at different stages. These different stages perform different functions. The scam emails which contain these strategies are usually in the form of narratives. For instance, in lottery scam, the recipients are sometimes told to fill in a form because they have won a lottery. This study was more focused on scam emails in the form of narratives which are centered on the scammer's personal life experience.

In sum, the studies reviewed above have provided knowledge on the discourse strategies employed in scam emails. The studies on discourse strategies in scam emails demonstrate that scam emails generate emotions and affections. The review also demonstrated that there are some similarities between business genre and scam emails. Also the review demonstrated that scammers possess technological and cultural abilities. The fraudsters, however, lack linguistic abilities which were revealed in the grammar, spellings and punctuations of their content messages. Also, scammers employ some persuasive techniques such as solicitation, extraction, irritation and appeal to manipulate recipients.

2.6.3 Rhetorical Structure of Scam Emails

In addition to discourse-pragmatic strategies, some studies have also examined the rhetorical structure of scam emails. Freiermuth (2011) studies rhetorical moves in 419 email messages to determine the main features that trigger receivers to give out valuable properties and monies. A total of fifty-two (52) 419 emails sent to one recipient were used as data in this study. The study concentrated on 419 emails that were in the form of narratives of experience and trust. The 419 narrative emails were then divided into three major groups: (i) dormant account, (ii) rescue operation and (iii) charity. The following moves were identified the in 419 email messages. (1) Opening salutation, (2) Establish personal/professional credentials, (3) Soliciting the offer, (4) Tale, (5) Trust statement, (6) Establish historical credentials, (7) Detail the offer, (8) Confidentiality plea Urgency statement, (9) Invite further contacts, (10) Ends politely. All these moves were there for one specific reason. The reason was to win the receiver of those messages to act upon them and respond positively.

The focus of this research was on 419 emails which were narrating an experience. This means that other 419 emails which do not fall within this category were not considered.

Naksawat, Akkakoson, and Loi (2016) investigate the structure of Nigerian 419 scam emails. Fifty (50) Nigerian 419 scam were analysed in the study. The focus of the study was to bring out the communicative purpose of scam emails and also identify the persuasive strategies that scammers employ to win the confidence and trust of the recipients. Each of the moves has sub-moves under it. The findings realised there were eight moves and fifteen steps in scam email messages. They are listed below.

Move 1: Providing an opening salutation

Move 2: Opening an email

Move 3: Introducing a purpose

Move 4: Phishing

Move 5: Requesting further action

Move 6: Ending an email

Move 7: Providing a complimentary close

Move 8: Providing a signature block

The findings identified four out of the eight as compulsory moves in scam email (1, 3, 7, and 8) and four others were optional moves (2, 4, 5 and 6). The compulsory moves were identified in all the fifty samples used for this data. For this reason, the researcher saw those moves as an important element which cannot be eliminated from the scam emails. The optional move, on the other hand, was not identified in all samples; this means the scammers can decide to leave them out but still achieve their communicative purpose in the messages. Moreover, the findings show that the internal structure of the 419 scam emails looks similar to that of the business English emails.

Mehrpour and Mehrzad (2013) examined the difference between English business emails written by Iranian business negotiators and Native English communicators. Thirteen Iranian business emails and 21 native communicators' emails were used for this study. The structure of business emails portrayed four compulsory moves in business emails. They are stated below.

Move 1. Establishing the negotiation chain

Move 2. Providing information/answers

Move 3. Requesting information/action/service/favours

Move 4. Ending

These four compulsory moves were employed in both the Iranian business emails and local communicators' emails. The difference between the Iranian and native English emails was found in the steps under each of the four compulsory moves.

The studies on rhetorical strategies in scam were mostly concerned with the moves employed by scammers to carry out their deceptive intentions. The review has discussed the various moves employed and the communication function of each move in scam emails.

2.6.4 Other Studies on Deceptive Strategies in Discourse

This section proceeds to discuss studies on deception detection in text types and discourses other than scam emails. The review here covers studies on discourse-pragmatic strategies (Section 2.6.2.1) and those on lexicogrammatical features used in deceptive contexts (Section 2.6.2.2).

2.6.5 Discourse-Pragmatic Strategies Identified in Deceptive Discourses

In addition to studies on scam emails, other studies have explored discourse-pragmatic strategies used in deceptive discourse across different contexts such as business and finance, online profiles, dating websites and verbal communication.

Humpherys et.al. have investigated the linguistic difference between fraudulent and non-fraudulent Managements Discussions and Analysis Sections (MD&A). Management Discussion and Analysis sections contain a company's records on how well they performed financially annually. Two hundred and two publicly financial disclosures were analysed.

The findings show that fraudulent Management Discussions and Analysis Sections contain more active language than non-fraudulent Management Discussion and Analysis Sections. This is so because managers usually exaggerate the success of their companies and rather conceal the negative aspects of their companies. Moreover, higher lexical word diversity and content word diversity were more in non-fraudulent Management Discussion and Analysis sections than fraudulent Management Discussion and Analysis sections. However, both had no difference in function word diversity. Longer words and more pausality were found in fraudulent Management Discussion and Analysis sections. But sentence length did not vary. This study helps to detect the linguistic cues of deception. However, the person who prepared such documents and the roles such a person played was not considered.

Toma and Hancock (2012) also did a study about online dating deception using the Linguistic Inquiry and Word Count (LIWC) approach. The study was in two parts. The first part analysed the textual self-description of online profile using a computerised linguistic analysis while the second part employed human coding on textual self-presentation.

The findings support previous studies which portrayed self-presentation as a holistic approach to detection of online deception. However, the study concentrated on only statements or information which was considered deceptive and does not take into account the context in which the deception occurred. The two studies further revealed that technological advancement has an impact on online deception. Online daters were able to make amendments in their online profiles on the information. This study is in line with Buller and Burgoon's (1996) interpersonal deception theory, which revealed that liars manage both the verbal and nonverbal aspects of the information in order to

avoid detection. The findings were categorized under twelve linguistic variables, which were of interest to the researchers. Some of the results of each variable were analyzed as discussed below.

Firstly, more deceptive words were produced in deceptive discussion than during truthful discussions. Both liars and their targets used more words when lying and no motivation effect was observed. Both liar targets produced the same number of words when it was truthful. Secondly, the targets used fewer words per sentence when lying. Thirdly, Liars used more question marks during deceptive communication. Fourthly, few first person pronouns were used when lying and there was no motivation effect. Fifthly, the research also observed that there was no increase in negative emotion terms during deceptive conversation. However, liars produced more negation words during deceptive discussions. The data of this study dispute previous assumption that liars avoid distinction markers. It rather suggested that unmotivated liars may increase the use of simple negation terms during deceptions. The findings also helped us to know that the target of the liars were unable to detect deception, though they both produce a different linguistic profiles during deception. This study is similar to Zhou et.al (2004), which also identified that deceptive senders produce more words than truthful ones. Moreover, deceptive senders avoid much use of self-reference pronouns. They rather distance themselves from the message sent or prefer group reference.

Mihalcea, Pérez-Rosas, and Burzo (2013) concentrated on deception detection in verbal communication using deception videos. The main aim of the study was to examine the deceptive strategies which were identified in the linguistic component of

the deceptive video and also to assess the difference between spoken and written deception statements.

The findings revealed that written and spoken deceptive statements have different features. It also revealed that the written data give more details than spoken data. The criteria used to study these videos may not apply to all people. Some people may speak with a feature which seems deceptive, but in actual fact they may be telling the truth. The videos are not enough to say one is deceptive or truthful.

Pérez-Rosas et al. (2015) studied linguistic and gesture features that are deceptive using real life videos. The videos were collected from public real-life trials and interviews, television shows and interview. One hundred and eighteen (118) videos were sampled for this study. Fifty-nine of the videos were labelled deceptive and 59 truthful. Elan software was used to transcribe the videos in order to study their linguistic features of deception.

The finding showed that nonverbal features, such as facial expression and hand gesture can help detect deception. Facial expressions such as side turn, up gaze, blinking, smile, lips down, open mouth, single hand, closing eyes, raising eyebrows and side tilt were identified.

Hildebrandt (2015) applied the survey approach to study the perception of online and non-online dating. The survey helped to know that online dating serves as a form of entertainment for online daters, while non-online daters fear dating online for several reasons such as lack of trust and discomfort. In this study, the participant may give accurate and adequate information useful for the analysis. Because some people usually wants to keep their dating life private. This may affect the accuracy of the data analysed.

Hauch, Blandón-Gitlin, Masip and Sporer (2015) investigated the validity and usefulness of computer tools used to detect deception in verbal accounts. Forty-four studies on deception detection were used as data for their study. All the studies considered for this study is analysed with a computer software. The study was in three parts. The first part examined descriptions of an attitude towards an event or a person the participants liked. In the second part, participants were asked to describe personal life events from the first person point of view. The third part involved problem solving or performance of a task by participants.

The findings demonstrated that liars tend to use fewer words, as well as few content and distinct words than truth tellers. This is because telling a lie is more cognitively demanding. Fewer exclusive words were also used by liars than truth tellers. This was so because it made their story simple and easy to understand. It was also noticed that liars edited their errors well in written texts to avoid contradictions. Tentative words were also less in deceptive accounts than truth accounts. However, negative utterances were preferred by liars. Hauch et. al. (2015) concluded that computer software can help detect deception in verbal accounts. This study concentrated on only studies that used computer software to analyse their data, which makes it limited. Other studies which have been useful in detecting deception but did not use computer software in analysing their data were not included. Also, since the data were collected from varied articles, the studies used different participants and approaches. This makes it difficult to get a uniform data on with same participants in the same environment.

Yoo and Gretzel (2009) studied the strategic use of language in deceptive and truthful hotel reviews. The data was collected from a group of marketing students in the

United States of America and *TripAdvisor.com*. A total of forty-two (42) deceptive hotel reviews and forty (40) truthful hotel reviews were collected and analysed for this study.

The findings demonstrated that hotel reviews come in various forms and shapes considering the length. The findings also demonstrated that there are no differences between deceptive hotel reviews and truthful hotel reviews in terms of quantity. The study also demonstrated that deceptive hotel reviews contained more complexity than truthful hotel reviews. Deceptive hotel reviews also made self-reference more than the truthful hotel reviews. It was also noticed that deceptive hotel reviews mentioned the brand names more than the truthful hotel reviews.

2.6.6 Lexicogrammatical Features Identified in Deceptive Discourses

Zhou, Twitchell, Qin, Burgoon, and Nunamaker (2003), studied cues deceivers use in a textual computer mediated communication. Sixty undergraduates participated in this study (34 females, 24 males). The participants were native speakers of the English language. The data were collected within four days.

The findings revealed that deceptive senders used more words, verbs, noun phrases and displayed less lexical diversity and content diversity. Also, deceptive senders made less self-reference and used more group reference and modal verbs in non-immediacy contexts. Moreover, the senders displayed more negative effect and emotiveness than receivers. The findings also showed some salient cues that deceivers employed in textual computer-mediated communication. Deceivers make dominant use of ellipsis, wordy sentences, and passive voice construction. Increased uses of second person pronoun and possessive forms were also identified.

Hancock, Curry, Goorha and Woodworth (2007) focused on the linguistic behaviour of both liar and the target of the liar during synchronous computer mediated communication in a deceptive and truthful situation. The study went further to examine linguistic changes in liars when they had a belief that they would succeed in their deceptive. In this study, the researchers analysed 246 transcripts using the Linguistic Inquiry and Word Count (LIWC) approach. The variables analysed included word count, word per sentence, question marks, first person singular pronouns, second person pronouns, third person pronouns, negative emotion words, exclusive words, negations, causal words and words pertaining to the senses.

Choudhury (2014) conducted a study on deception detection in a criminal suspect interview from a forensic linguistic perspective. The study investigated linguistic cues of deception in an interview of a suspect who murdered her boyfriend and was found guilty. The linguistic markers of deception such as lack of commitment to a statement and preference for negative forms were dominant in the study. Other linguistic markers, such as sense words, other-oriented pronouns and references, and speech disfluencies were explored as well. The findings revealed the murderer made use of equivocation which revealed that she lacked confidence. The equivocation manifested in the dominant use of non-factive verbs. The murderer also made a lot of vague construction and did not give specific content during the interview. Negation usage was almost significantly, seen in her use of contracted negation, negation quantifier pronoun, negative morpheme, negative-emotion. The murderer also displayed a lack of memory to avoid interrogations which were more challenging. Sense words were also prominently used by the murder in order to persuade the interviewer to believe her. Sense words were also dominantly employed during the interview of the murder. The murderer tended to display speech disfluencies in order to conceal some vital

clues as well. The linguistic markers identified in the transcript of her speech revealed that her message was deceptive. This also means that linguistic markers are effective tools for the detection of deception. This study was significant in detecting deception in language from the forensic linguistic perspectives.

Afroz, Brennan, and Greenstadt (2012) conducted a study to identify deceptive documents from regular documents. The data were collected from Ernest Hemingway and William Faulker imitation contest. Another set of data were taken from Brennan-Greenstadt dataset and Thomas-Amina's Hoax corpus. Sixty-eight articles were sampled for this study. Three class classifications (regular, imitation and obfuscation) and three feature set (write-prints feature set, lying-detection feature set, and 9-feature set) were employed in this study. This study explored these three feature sets employed in order to identify deception in stylistics. The study concentrated on the three write-prints feature set, that is, lexical, syntactic and content specific features. Linguistic Inquiry and Word Count terms were employed in the lying-detection feature set. The terms are quantity, vocabulary complexity, grammatical complexity, uncertainty, specificity and Expressiveness, verbal non-immediacy. The features examined in the study are a number of unique words, complexity, grammatical complexity, uncertainty, specificity and expressiveness, verbal non-immediacy. The findings are discussed below.

First, the results showed that a classifier trained on sets of adversarial and non-adversarial documents can detect deceptive documents with 96% accuracy using their feature set. Also, there was no clear cut difference between content-specific and non-content-specific features in detecting deception. The difference was realised on the function words. Moreover, there was a dominant use of the existential 'there' and

adverbs in obfuscated passages. Personal pronouns were also dominantly used. Furthermore, the findings posited that there are no distinguishable features of deception and lying as they both possess similar features. To add to the above, obfuscation was harder to detect than imitation.

The data analysis were limited to only three set features, probably if the data was widely opened and not restricted to any set features, a different finding could be derived which would be interesting. But if the data was categorised around three set features, any finding which does not fall within that range would not be considered as important. The specific pronoun used was mentioned, that is, personal pronouns. However, the findings were grouped under broad headings, such as verbs, adverbs and function words without necessarily telling the reader the kind of specific verb or adverb type used.

In sum, the review in this section has demonstrated that both the liars and the target recipients have roles to play in deception. Also the review indicated that personal pronouns were dominantly used in deception. However, deception senders use less self-reference pronouns. Moreover, liars produce more and are motivated to write more when they receive a reply from their target recipients. The review also demonstrated that the liars manage their verbal ability well to avoid detection.

2.7 The Relationship between Previous Studies and the Present Study

The review above shows that the language of deceptive discourses has been studied from different perspectives in the linguistic literature. In summary, studies have examined the discourse-pragmatic strategies, the rhetorical structure and the lexicogrammatical features of deceptive discourses. Various theories and methods have also been used, notably the Criteria-Based Content Analysis (CBCA), Linguistic

Inguiry and Word Count (LIWC), Reality Monitoring (RM), Scientific Content Analysis (SCAN), Verbal Immediacy (VI), Strategies and Tactics, and the Interpersonal Deception Theory (IDT) (cf. Fuller, Biros, Burgoon, & Nunamaker, 2013; Zhou et al., 2004). A number of gaps can be identified in the literature. First, while most of the studies are on the discourse-pragmatic strategies used in deceptive discourse, only a few studies examine lexicogrammatical features. As the review shows, lexicogrammatical studies are particularly lacking for scam emails. Lexicogrammatical studies on deceptive discourses, in general, and scam emails, in particular, are however important in revealing hidden and underlining strategies of scam. Second, studies on the lexicogrammatical features of scam emails have focused on a few linguisitc items such as pronouns, negative words, emotion words and lexical complexity. There is still the need to undertake a holistic analysis of whole text processes in order to get a comprehensive understanding of the linguistic construction of deception. The present study is intended to fill some of these gaps. It gives a clause by clause analysis of scam emails in order to examine how the lexicogrammatical system of transitivity is used in representing deception in discourse and in manipulating the target of scam email recipients.

2.8 Theoretical Framework

This section will proceed to discuss the theoretical framework underlining the study. It will first examine the systemic functional theory, which is the general theory for the study, and then continue to discuss the system of transitivity, which is the particular lexicogrammatical system used in analyzing the data.

2.8.1 Systemic Functional Theory

This study is guided by Systemic Functional Linguistics theory (SFL). SFL is a theory of language which was developed by Michael Halliday (cf. Halliday, 1961, 1966; 2008; Matthiessen, 2007; Martin, 2016; Mwinlaaru & Xuan, 2016). This study is guided by two dimensions of Systemic Functional Linguistic (SFL), that is, "system networks" and the notion of metafunctions of language (Halliday, 1985, 2006; Halliday & Matthiessen, 2004; Halliday, Matthiessen, & Matthiessen, 2014). SFL is considered as both systemic and functional. Systemic means that there are a set of linguistic choices available to language users. These set of linguistic choices are interrelated (to one another) in meaning. The choice of a specific linguistic feature is influenced by the whole of the linguistic system (Halliday et al., 2014; Thompson, 2013). The system is considered as the means of meaning in language. The main distinctive characteristic of system theory is that "a language is a resource for making meaning" and that "meaning resides in systemic patterns of choice" (Halliday and Matthiessen, 2004, p. 23). Language as a resource for making meaning means speakers have the opportunity to choose from the varied linguistic items presented to them based on the purpose one wants to achieve using language. That is, when speaking, one uses specific words in order to achieve a particular function.

Martin (2016) gives reasons why SFL is considered functional, that is, it gives the distinctive feature between word function and word class. He further shows that the word class and function distinction make it possible to see the different functions performed by a certain word class. Language is used to perform various functions. Halliday and his team of researchers (Halliday and Hassan 1976; Halliday 1985; Halliday and Mathiessien 2004, Halliday and Mathiessien 2014) group the main function of language into three namely, the ideational, interpersonal and textual

function. The three functions mentioned above are collectively called the metafunctions of language. The three metafunctions of language are discussed below. Ideational meaning considers the clause as a way of expressing our beliefs, thoughts, ideas about things revolving around us in both the physical surround and inner world of the mind. The ideational meaning is realised in the clause basically through the transitivity system. Interpersonal meaning is realised through the mood and modality. Textual meaning relates the meaning of an oral or written discourse to the environment and situation in which such a discourse is employed. Textual meaning is realised by theme and focus of information. This study is centered on the ideational meaning. The main means of understanding the ideational meaning is through the transitivity system. The concept of transitivity is discussed below since transitivity is the main analytical framework which will be used to explore the language of scam in this study.

2.8.2 The Concept of Transitivity

Systemic Functional Linguistics (SFL) is the main theory guiding this study and Transitivity is the analytical framework used to analyse the language of scam email messages. Transitivity is the means by which the meaning of experiences and happenings are expressed through the use of the clause. (Halliday and Mathiessien 2014). The clauses in which the experiences are represented usually contain three primary components. The process, which is expressed by the verb. The process is considered as the main central idea of the clause which is expressed through time (Downing & Locke, 2006). The participant, which is represented by a noun phrase and the circumstance, which is usually represented by the adjunct. The circumstance gives additional meaning to the clause.

Transitivity is also identified by Halliday and Mathiessen (2014) as a lexicogrammatical system that indicates how language represents experiences. The system consists of six process types, namely material processes, mental processes, relational processes, verbal processes, behavioural processes and existential processes. Transitivity is a semantic as well as a grammatical concept in nature. This means, transitivity accounts for the meaning of experiences using the grammar of the language. Thompson (2013) advocates that the main means of understanding the meaning associated with the clause is through the process types. Transitivity consists of three main process types, namely material, mental and relational. There are three subprocesses under the three main processes, the verbal, behavioural, and existential. Halliday and Mathiessen (2014), notes that the three sub processes are not whole processes on their own, but proceed from the three main processes.

The material process is the process which involves physical actions and events. It is the most dominant of the process types and has varied sub types which can be subcategorized into different groups. Thompson (2013), states that all material processes have an actor. Sometimes the actor is not visible in the clause, but it does not mean there is no doer. The actor is implied in the clause. Material processes can be grouped into varied sub categories as mentioned earlier. The processes can cause an entity or things into existence, in other words, make something which does not exist come into existence. The material processes can do this by creating that entity or by calling it into existence. Sometimes, the material processes can do something to an existing entity or thing to transform it from one state to another. Thompson calls these two subcategories creative and transformative respectively.

There are two important participants in the material processes, that is, the actor and the goal. The actor is the entity that performs an action in the clause while the goal is the entity the actions performed by an actor affects. In other words, the actor is the doer of the actions in the clause while the goal is the one the actions are aimed or directed at. Halliday identifies other participants, which are related to the material processes. They are the initiator, scope, client, recipient and attribute.

Mental process deals with the experiences of a person's inner world. Mental process represents thinking, feeling and wanting. Downing and Locke (2006), mentioned that it is not everything that is expressed by acting it out. It can be done internally without showing or executing an action. In other words, it deals with the experiences that take place in the mind. Mental process also has sub categories just as the material processes. Four subcategories of the mental process are identified, namely, emotional, noticed in verbs such as love, admire and like. Cognition realized in verbs such as know, understand, believe, forget. Perception which realized in verbs such as feel, hear, notice, taste and desideration; hope, want wish and desire (Downing and Locke 2006, Halliday & Matthiessen 2006, Thompson 2013,). The two participants associated with the mental process are the senser and the phenomena. The senser is the one who is sensing an entity and the entity he is sensing is the phenomena.

Relational process is the last dominant process of transitivity. Relational process is quite different from the material and mental. Relational process deals with the relationship that exists between entities. Relational process represents possession, attribution, and identification. There are different categories of relational process, that is, Attributive and identifying relational process. The attributive is concerned with the state of an entity, thing or a person while the identifying category shows the objective

or motive of an entity. The relational process could also be circumstantial or possessive in nature.

Verbal process is a minor process type in transitivity. Verbal process lies between the material and mental processes. The verbal process is the manifestation of what is going on in the mind through physical actions. Verbal processes represent saying. On that note, there are four participants related to the verbal process. Sayer, the one who says something, receiver, the one the saying is addressed to, the target, the one the message is aimed at and the verbiage, the content of the clause or what is said in the clause.

Behavioural process is the borderline between mental and material processes and is represented by verbs such as cough, sneeze, yawn, blink, laugh and sigh. Behavioural process represents behaving. According to Downing and Locke (2006), the behavioural processes are usually involuntary. Behavioural processes have two important participants, which are the behaver and range also known as behaviour. The behaver is the one who elicits the act while the range is the behaviour elicited.

Existential process is the process of existing of an entity or happening. The existential states the existent of an entity and also specifies the location of the existence (Downing and Locke 2004). Existential process represents existence and has one main participant, which is the existent, that is, an entity that exists.

Table 2.1: Summary of Process Types and Their Category Meaning and Participants

Process Type	Category Meaning	Participants, directly involved	Participants, obliquely involved
material: action	'doing'	Actor, Goal	Recipient, Client; Scope; Initiator; Attribute
event	'doing' 'happening'		
behavioural	'behaving'	Behaver	Behaviour
mental:	'sensing'		Senser, Phenomenon
perception	'seeing'		
cognition	'thinking'		
desideration	'wanting'		
emotion	'feeling'		
verbal	'saying'	Sayer, Target	Receiver; Verbiage
relational:	'being'	Carrier,	Attributor, Beneficiary
attribution	'attributing'	Attribute	Assigner
identification	'identifying'	Identified, Identifier; Token, Value	
existential	'existing'	Existent	

Source: Halliday & Matthiessen (2004, p. 260).

2.9 Application of Systemic Functional Linguistic to the Present Study

Applying the SFL approach to the present study means that, first, the analysis of data takes into consideration the whole system of transitivity as well as the environment in which those words occur must be linked to the description. Second, the analysis will go beyond the basic structure of the clause and look at the purpose and context of scam emails in interpreting the findings. Next, SFL theory indicates that language is a theory of human experience and every domain of experience has particular ways of using language. Since transitivity is the major grammatical system for representing experience, the present study investigates how the resources of transitivity are used in constructing deception in scam in order to manipulate the targets of scam.

2.10 Summary of the Chapter

This chapter has reviewed literature related to the present study. Theoretical and empirical studies relevant to this study were the main focus in this chapter. The first part of this chapter reviewed discourse strategies in scam emails, rhetorical structure in scam emails and other studies on strategies of deception focusing on the discourse-pragmatics strategies which were relevant and related to this present study. The lexicogrammatical features identified in the deceptive discourse were also discussed. The study then demonstrated the relationship between previous studies on deception and the present study.

The second part of this chapter also discussed the theoretical framework used in this study, that is, the Systemic Functional theory, paying particular attention to its notion of system network and the three metafunctions of language. The concept of transitivity, which is the analytical framework for this study, was also discussed in this chapter. The chapter then demonstrated how Systemic Functional Linguistics can be used to explicate the present study. The next chapter demonstrates the methodologies employed in this study.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

The preceding chapter reviewed literature related to the study of deception. It considered the theoretical framework for the study, as well as some relevant empirical studies related to the study. The present chapter discusses the methodologies employed in this study. The chapter discusses the research methodologies. These include the research design, source of data, data collection procedure, and procedure of data analysis.

3.1 Research Approach

This study employs the qualitative research approach. Hancock, Ockleford, and Windridge (2007) note that the main focus of qualitative research is to explore the world we inhabit and why certain behaviour happens. This study analyses the language of deception in order to interpret the meaning of scammer's language. Creswell (2013) believes that qualitative research deals basically with the meaning of the data. The present study also focuses on how to construct meaning out of the data under study. The choice of the qualitative research is also in line with Altheide and Schneider's (2012) assertion that qualitative research aims at an understanding of the document under study and relates the issues identified in the text to theories.

The study of online behaviour has become necessary as people now use the internet for their daily activities. This study therefore examined the attitudes of people on the internet using text as the reference point. Hallet and Barber (2013) argued that the study of the behaviour of people in their natural environment should include the use of online to explore the lives of such people online. The internet now allows people to

communicate with individuals, institutions and organizations on a daily basis and therefore constitutes an aspect of their personal life (Herring 2004). Since this study is on email scam, all the scam email messages that constitute the data for this study were derived directly from the internet.

3.2 Source of Data

Chapelle (1998) believes that systemic functional linguistics is a text oriented theory. Halliday (2004, p: 33) posits that "text is the form of data used for linguistic analysis; all description of grammar is based on text". As mentioned earlier, this study examines the linguistic construction of deception in scam emails. The scam emails were accumulated from the researcher's own email, solicited from various recipients and http://www.419scam.org. This website was chosen because it is a recognizable site where different scam emails are posted for viewers to beware of. Only emails written in English were selected for the study.

The social science research technique of saturation point was employed in collecting and analysing data. This principle allows the researcher to keep on analysing data until the data yield no new results (Patton and Cochran 2002). Thus, the analysis for the present study stopped at forty scam email messages, since the data was longer producing any new patterns of the occurrence of process types or new patterns in their frequency distribution. One implication is that scam emails share very similar characteristics and are recurrent in their organization and linguistic features. The present study is concerned with these recurrent patterns so far as transitivity is concerned.

3.3 Data Collection Procedure

The purposive sampling technique was used to select the specific scam emails used for the analysis in this study. The choice of the purposive sample technique was influenced by the type of data used for this study, which is a scam email message. My intention was to look out specifically for emails which were meant to deceive recipients in order to gain money or a favour. So in this regard, the purposive sampling technique was found to be the most appropriate as it allowed me to pick and choose emails with scam features in particular. I concentrated on scams that span from January 2016 to December 2016. The year 2016 was chosen because of its recency. I wanted to have scam emails sent to recipients within the same year so they would be used as representative of all scam email messages sent within the year. The emails ranged between half a page and two pages. None of the scam email messages selected for this study went beyond two pages. The scam email messages used for this study were organized into seven main categories. The seven main categories were: dormant account, charity, business transactions, lottery win, rescue operations, free shopping and account update. The samples in each category were considered generally a representation of that particular category of scam email messages. Table 3.1 below contains illustrations of the seven various categories of scam email messages used for the analysis in this study.

3.4 Types of Scam Emails

This section discusses the type of scam email messages used for this study before proceeding to the analysis of the data. This is important to contextualize the transitivity analysis. Scam emails contain no much difference based on the types (Rich 2015). In this study, the data also revealed no little difference between the types of scam email. The main purpose of the scam emails was to solicit personal

information about the recipients (Holt and Grave 2007; Edelson, 2003). But the scammers would not ask for the recipient's identity because, it would not be given. They therefore make up these stories to get the information they need. Therefore, scam emails were categorized based on the content of the text for the purpose of this study. Seven categories (dormant account, charity, lottery win, business transaction, rescue operations, shopping and account update) of scam email messages types were identified. After identifying the scam emails into classified category, a quantitative count was given in table 3.1 below. A brief description of each category is given below.

3.4.1 Dormant Account

The scammers usually start with greetings and then proceed to introduce themselves. The scammer usually poses as banker, attorney or lawyer of a foreign national who had pass away in a tragic accident or illness. The owner usually has no beneficiary but has a huge sum of money in his or her account. The account is now dormant. The scammer therefore wants the recipient to help him get the money for their mutual benefit. The scammer usually demands confidentiality between him and the recipient.

3.4.2 Charity

The scammer poses a devout Christian or a sister who is suffering from cancer or a strange sickness. He or she therefore needs someone who is also a devout Christian to transfer all his funds to him in order for the money to be used as charity.

3.4.3 Lottery Win

The scammer gives the recipient the information that he has won a lottery which involves a huge amount of money. The recipient therefore has to provide some vital details of his account for the money to be transferred to him or her.

3.4.4 Rescue Operation

The scammer poses as someone who has got into trouble in his or her homeland and needs to get his or her family and funds out of the country. He or she therefore wants to transfer the funds into the account of the recipient and also send his family along. He will then follow later. The recipient is promised a percentage of the money as a reward.

3.4.5 Business Transactions

The main aim of this type of message is to persuade the recipient to enter into a partnership with the recipient in an investment project.

3.4.6 Shopping

The scammer gives the recipient a free gift offer on a shopping site or shopping centre. The recipient is instructed to enter some details of his/her credit card to qualify for such offers.

3.4.7 Account Update

This type of scam email usually instructs the recipient to update his or her bank account information or software he or she is using. The recipient has to update the account by providing vital details. Sometimes, the recipient is given a discount if he updates a credit card or software.

Table 3.1 Distribution of emails in the data across different categories

Category of scam	Number of messages
Dormant accounts	8
Charity	6
Lottery win	3
Business transaction	13
Rescue operations	2
Free shopping	5
Account update	3
Total	**40**

3.5 Data Analysis

This study employed Burton (1982) method of transitivity analysis (see Simpson, 2004, p. 189). This method helps to clearly identify the processes and identify their discourse effects. It also helps to know which roles participants play and who is affected most in the text. The procedure is summarized below (Simpson, 2004, p. 189):

> (1) isolate the processes, and find which participant (who or what) is 'doing' each process;
>
> (2) find what sorts of processes they are, and which participant is engaged in which type of process;
>
> (3) find who or what is affected by each of these processes.

The relevant email messages were downloaded and sorted for this study. The messages were then saved on Microsoft word sheet. The sorted emails were then printed out and studied to see the transitivity elements in them. The texts were read repeatedly to identify the clauses types. The messages were coded manually, and chunked. After that, the chunked clauses were typed and migrated to Microsoft excel sheet and edited for easier sorting and identification of process types. The sorting and the identification of the process types were done several times on different Microsoft excel sheets to see if there was any variation (in each of them involved) in each process type identified. The specific type of process was then identified and labelled. The analysis concentrated on the content of the texts only. There were greeting and salutations features in almost all the scam email messages but they were not considered in the analysis. Greetings and salutations are considered minor clauses in

the sense that they are one dimensional in function. They only perform an interpersonal function (Halliday & Mathiessen 2014).

The data was continuously edited even when work was ongoing to correct any errors identified. The researcher was sometimes confused in categorizing clauses into the process type. Confusing clauses and samples of the analysis were given to a Ph.D. candidate and an MPhil student in systemic functional linguistics for verification and clarification. Sometimes too, I had to resort to the text books or analyses done by other scholars for clarification.

The study employed the frequency count and struck percentages in order to answer the first research question. The frequency of occurrence of each process type with it percentage was presented in a tabular form. In relation to research question two (2), the roles performed by participants and their associated circumstances were identified. After identifying participant roles, the patterns of the various process types were identified and analysed.

3.6 Summary

This chapter has discussed the methods and techniques employed in collecting and analysing the data. The chapter has discussed the research design, the source of data, data collection procedure, types of scam emails used for the study and the procedure for data analysis. The next chapter presents the analysis of the data.

CHAPTER FOUR

ANALYSIS AND DISCUSSION

4.0 Introduction

As mentioned earlier in Chapter 1, the aim of this study is to investigate how deception is construed in scam emails using transitivity as an analytical framework. The two preceding chapters examined theoretical issues related to this study, the empirical studies related to the discourse of online deception and methodologies employed to carry out this study. The present chapter presents the findings of the study according to the research questions stated in Chapter 1:

1. What process type(s) is/are used in scam emails?
2. (a) What transitivity pattern(s) is/are used in scam email messages to construe fraud?

   (b) How do they reveal the manipulative purpose of scamming?

4.1 Process Types used in Manipulating Recipients of Scam Emails

There were various process types identified in scam email messages. Table 4.1 below presents the quantitative counts of the six process types of transitivity, namely, material, mental, relational, verbal, behavioural and existential. Table 4.1 is used to answer research question one (1). The process types and their frequencies, as well as their percentages are the main focus of discussion in this section.

Table 4.1: Distributions of Clauses in Scam Emails across Process Types

Process type	Frequency	Percentage (%)
Material	442	51.4
Relational	241	28.0
Mental	127	14.7
Verbal	44	5.1
Existential	3	0.4
Behavioural	3	0.4
Total	**860**	**100**

The data showed that material process types were dominant in the scam email messages. A total of 442 material process types were found in the scam email messages analyzed, representing a percentage of 51.4% of the total number of clauses. This implies that more than half of the clauses analyzed were material processes. The second most frequent process type was the relational process type. The relational process types recorded are 241, representing a percentage of 28.0%. The mental process type was the third frequent process type found in the clauses. It occurred 127 times (i.e. 14%). The verbal process type was the fourth frequent process type, with a frequency of 44 (5.1%) of the total number of clauses. The existential and behavioural process types occurred least in the scam email messages. They each had a frequency of three, representing a percentage of 0.4%.

The high occurrence of material processes reveals that scamming via email represents more of actions and happenings than other domains of experience. The scammers recount a series of actions in the scam email messages and also instruct the recipients to undertake particular actions in order to yield a successful outcome. In other words, scammers tend to focus more on recounting activities and happenings as well as the activities they desire their targets to engage in. As indicated in Table 3.1 (cf. Chapter 3), most of the scam emails in the data set belong to the business transaction category. Generally, the frequency distribution of clauses across process types in the scam

email messages is not marked when we compare it to the typical distribution of process types in English discourse. In a quantitative corpus study of process types in English, Matthiessen (2007: 812) reveals that across different registers, the most frequent process types are material, relational and mental, in their respective order of frequency. These are followed by verbal, behavioural and existential, which is the least frequent process type (see also Halliday & Matthiessen, 2014: 215). This frequency distribution of process types is corroborated by this study as Table 4.1 shows. The implication is that scammers do not markedly favour any particular selection in the system of process types in their emails. However, it still remains that scam emails represent more of actions and happenings, sensing and having-&-being than other domains of experience. Scammers use these process types that also occur in everyday discourse as manipulative linguistic strategies to lure their targets. The use of each process type as a manipulative strategy is discussed in the following section (4.2).

4.2 Transitivity Patterns used in Manipulating Recipients of Scam Emails

Numerous definitions have been given by scholars as to what constitutes a pattern, but Hunston's definition of a pattern in language guides the analysis of pattern in this chapter. Hunston (2010) indicates that a linguistic pattern is realized when words, sounds, rhythms or structures are replicated. Since this study also discusses the repetition of patterns in scam emails, Hunston's definition is appropriate to guide the study. The use of each process type as a manipulative strategy in scam emails is discussed below.

4.2.1 Material Process Type

From the analysis, it was observed that the material process recorded the highest frequency of occurrence in scam email messages as shown in table 4.1 above. A

detailed analysis of the patterns identified in the material clauses of scam email messages are discussed below with illustrations from the text.

The transitivity patterns of the material processes in scam email messages indicate that the scammers variously position themselves as negotiable, vulnerable and generous. There were various actors associated with material clauses. Nonetheless, personal pronouns were predominantly used as Actors. Casañ-Pitarch (2016) posits that personal pronouns give writers the opportunity to make their writings lively and also to make it easier for readers to understand the subject and see it as personal. This could be the reason why the scammers use personal pronouns to make the reader understand their message easily since the easy understanding is what will trigger the recipients to respond. The personal pronouns used as Actors include 'I', 'you', 'he', 'she', 'they' and 'it'. The most used personal pronoun was 'I' and 'you' which reflects the fact that the emails were interpersonally rich. However, the scammers employed 'I' as Actor more than any other pronoun, putting the scammers in control of the semiotic process involving writers and target readers. The material clauses illustrated below are used to explain this point further:

1. I (Actor) 'm writing (Material) to let you know (Circumstance) that my family and I (Goal) are stuck in Madrid [STX02, CL1.0].

2. I (Actor) am writing (Material) this mail (Goal) to you with heavy tears in my eyes and great sorrow in my heart (Circumstance) and I (Actor) am contacting (Material) you from my country Tunisia (Circumstance) [STX11, CL1.0].

3. I (Actor) am writing (Material) this mail (Goal) on behalf of my client (Circumstance) [STX22, CL3.0].

4. I (Actor) selected (Material) you (Goal) to receive a cash sum of $1.500,000,00 USD (Circumstance) [STX23, CL3.6].

5. I (Actor) am contacting (Material) you (Goal) to negotiate my proposition for investment funding in your country (Circumstance)[STX24, CL2.0].

In the examples illustrated above (1, 2, 3, 4, and 5), 'I' is Actor in all the clauses. The scammers take responsibility as the author, the animator and the controller of the discourse. The clauses typically consist of the first person singular pronoun 'I' plus a material process with an associated circumstance. This gives the recipients an impression that the scammers are bonding with them. For emails in the category of business transaction, in particular, this *'I-orientation'* helps reduce bureaucratic distances in their negotiation and has the potential of making the transaction faster and smoother. In other words, this bonding strategy has the potential of motivating the recipients to give the scammed transaction a try.

Also, the personal pronoun 'I' was dominantly used, plus a material process and a circumstance of reason explaining why the scammers are writing the letters, as seen in examples (1, 2, 3, 4, and 5). The scammers show their negotiable attitude when they indicate their reasons for writing the letters in the circumstantial elements of the clause. These reasons serve as an attractive hook that would bait the target recipients of the emails to reply positively. In scam emails, therefore, scammers project themselves as negotiable and affable, presenting their message in the form of a proposal or a plea which the recipients are motivated to respond to.

Some of the circumstances associated with material process types also show that scammers mostly portray themselves as vulnerable. They portray themselves as someone being exploited or in trouble and the recipients will have to rescue them by responding to the email messages. Sometimes, the scammers portray themselves as someone who is about to die and needs the help of the recipients to fulfill his or her last wish. The scammers actually let the recipients know that without the recipient's

assistance, they may not survive or cannot deal with the issue alone. This is a manipulative strategy used by the scammers to gain pity from the recipients and also urge them to respond promptly as well. Such fake vulnerability is a strategy used by the scammers to manipulate scam email recipients.

The scammers also use material processes to portray themselves as generous by making attractive offers to target email recipients. The scammers also sometimes ask the recipients to give an opinion on how the transaction should be carried out. In example (6) below the scammer indicates that in case the recipient agrees to carry out the transaction, all the details needed to make the transaction successful will be provided. In example (7), the scammer made the recipient aware that he was purposely selected by him to receive such a huge sum of money. The scammers usually give the recipients a motive for writing such a letter. Such a motive could be for business transactions, charity or help to have access to a dormant account. Example (6) shows that the motive of the scammers was for them to enter into a business transaction while example (7) reveals that the scammer is offering charity to someone.

Tan and David (2017) noticed that in online dating fraud, the scammer mask his intention to the target. This means that whatever intention scammers indicate in the scam email messages is not the real intention behind those emails. The scammers usually give the recipients an impression that they are writing in order to enter into an attractive business negotiation with the recipient. A business transaction is about negotiation and this gives the recipients an impression that the message is genuine which explains why they could fall prey to such a plot, even though the main intentions behind the messages are to dupe recipients. The scammers are using a strategy to make the recipients believe that their intentions behind the transactions are

genuine and also to present their transaction as attractive to motivate the recipients to succumb to their deceptive thoughts and ideas.

> 6. I (Actor) shall give (Material) you (Receiver) the contact (Scope) of the bank in Burkina Faso (Circumstance) [STX22, CL6.0]
> 7. I (Actor) selected (Material) you (Goal) to receive a cash sum of $1.500,000,00 USD (Circumstance) [STX27,CL3.5]

Moreover, the scammers provide justification for their actions in the material clauses. Since scam email messages are sent to recipients without any prior relationship between the two parties, the scammers usually provide reasons why they contacted the recipients in such manner. They usually give circumstances surrounding the messages which compel them to send such mails without any prior relationship. This point was also highlighted in Freiermuth's (2011) study of rhetorical moves in scam emails, where the findings showed that scammers usually gave reasons for their actions in order to make them sound believable. The reasons the scammers provide for writing such letters may not be true, but they will give reasons to buttress their deceptive stories. Naksawat, Akkakoson and Loi (2016) also point out in their study that scammers explain the reasons behind the emails they send to the various addresses.

The scammers employ the Actor 'I' plus a material process and a circumstance to provide justifications for writing the email messages. The circumstantial elements in the material clauses usually contain all the justification needed for the recipients to understand the messages. In example (5) above, for instance, the scammers gave a reason for writing letters to the recipients. Other examples are highlighted below:

8. I (Actor) am suffering (Material) from Kidney cancer (Circumstance). I (Actor) won't live (Material) more than 2 months according to my doctors (Circumstance) [STX10, CL6.0]

9. I (Actor) am writing (Material) [[to bring to your notice about your compensation Bank check [[brought to white house by UNITED STATE EMBASSY in Cotonou Benin Republic]]]] (Circumstance) [STX03,CL2.0]

10. Permit (Material) me (Goal) to inform you of my desire of going into business family relationship with you (Circumstance) [STX03,CL1.0]

11. My partner Darren D. Braswell, 36, of Riverdale, Ga., (Actor) died (Material) Jan. 7th near TalAfar, Iraq (Circumstance), || when the UH-60 Blackhawk helicopter [[in which he was a Passenger]] (Actor) crashed (Material) [STX08,CL4.0]

In the circumstantial elements underlined in the examples above, (8, 9, 10, 11, 12, 13) the scammers are giving the recipients reasons for sending them such messages. The reason could be a matter of urgency which needs prompt attention and for that matter, the scammer usually contact the recipient without giving him or her prior notice as seen in example (8). The scammer explains to the recipient in example (8) that he is sick and may not live long and needs the help of the recipient to fulfill his last wish and that is why he contacted the recipient in such a manner. Example (9) carries important information about a check which had been brought to the bank on behalf of the recipient which the scammer wants to draw the target recipient's attention to in order to rectify any mistake as early as possible. Therefore, there was no time for the scammer to contact the recipient to negotiate before relaying such important information to him. In example (9), the scammer wants to go into a business partnership with the recipient, which is why he contacted him. Example (10) rather gives additional information as to why the scammer contacted the recipient. The

messages illustrated above carry some urgency in them and the scammers see it as important to contact the recipients directly without any prior relationship.

The material clauses reveal that the scammers assign responsibilities to their target recipients. It is observable from the data that though the scammers control the transaction, they also assign duties to other participants in the text to carry out. In cases where the scammers assigned duties to other participants, the participant is basically the recipient "you" plus a material process accompanied by a circumstance or Goal.

Instructions are given to those participants by the scammers. Sending of the recipients' personal information to scammers is one of the key actions the scammers want the recipients to carry out. This point is supported by earlier studies (Edelson 2003; Holt & Grave 2007; Smith et al. 1999) that indicate that scammers always send messages to recipients and expect them to give them feedback in the form of personal details. These personal details are means used to dupe the recipients. The basic aim of the scammers is to get vital information about the recipients.

The scammers therefore employ the participant 'you' plus a material process and a circumstance or Goal in scam email messages when they want the recipients to provide them with some vital personal information about themselves. The only way of gaining such information from the recipients is by assigning that same duty to the recipients because the scammers have no personal details about the recipients. They therefore use this strategy to get what they desire from the recipients without making it sound obvious. This shows that in order for scammers to carry out their deception successfully, the recipients have essential roles to play. The scammer's main duties are to send those messages but they cannot succeed if the recipients do not reply to such messages. The role of the recipients is therefore the most important element in

scam email messages. Hiß (2015) points out that scammers are supposed to be submissive to recipients but there are instances where the scammers command the recipients to act. Commanding the recipients to act usually comes at the stage where the scammers want the personal information of the recipients in order to manipulate the recipients. Even though the recipients may not see the command elements in the messages, the use of, imperative clauses gives the sense of command which may not be noticed by the recipients.

It was also observed in the analysis that the scammers employ the participant 'you' plus a material process and a circumstance which either direct the recipients to a website where the recipients are supposed to visit for more information about the transaction, as seen in examples (16, and 17) below. Examples (16 and 17) direct the recipient to a website where more information about the deal can be accessed. There are also instances in the text where the scammers also ask the recipients to send the vital information through a provided email address as seen in examples (12, 14, 15, and 18). Sometimes, the scammers ask questions which seek to elicit personal information as when the recipients are asked to complete a form with their personal information. Examples of material clauses which employed the participant 'you' plus a material process and a circumstance are displayed below.

12. You (Actor) send (Material) reply (Scope), to: sbaduesqgh@gmail.com (Circumstance) [STX40,CL3.0].

13. you (Actor) will utilize (Material) this money (Goal) the way I am going to instruct here (Circumstance) [STX11, CL10].

14. You (Actor) contact (Material) him (Goal) now on the email provided below (Circumstance) [STX39,CL6.0].

15. you (Actor) respond (Material) for further details. email: mr.martin.g2001@gmail.com (Circumstance) [STXO1,CL7.0]

16. You (Actor) can read (Material) more on this website for more information and explanations (Circumstance) [STX08, CL18]
17. You (Actor) will type sign (Material) on the website displayed [STX23, CL8.2]
18. You (Actor) can indicate (Material) your option (Goal) towards assisting me by replying to the email provided below (Circumstance) [STX13, CL5.0].

As these examples (12, 13, 14,15,16,17 and 18) above show, the scammers employ the personal pronoun 'you' plus a material process with a Goal and Circumstance of place or location to indicate what duties the recipients are supposed to execute. The scammers assign these duties to the recipients in the form of command, but the recipients do not notice it since it is not made so obvious.

Also, in the analysis, the scammers employ the implied participant 'you' plus a material process and a Goal or Circumstance to delegate duties to the recipients without making direct reference to the recipients. The scammers rather make a direct reference to themselves as the Goal in the text. In those instances, the participant 'you' was implied in the material clauses. The scammers do not mention the recipients, but a direct command is given. These direct commands contain the implied 'you' as seen in examples (19, 20, 22 and 23) illustrated below.

19. [you] (Actor) Contact (Material) me (Goal) for more details (Circumstance) [STX29,CL3.0]
20. [you] (Actor) contact (Material) me (Goal) with this Email:songchen29@hotmail.com (Circumstance) [STX30,CL5.0]
21. [you] (Actor) contact (Material) me (Goal) through my private email address mr.abraham@hotmail.ru with your full details as bellow, (Circumstance)[STX22,CL3.0]
22. [you] (Actor) Contact (Material) us (Goal) at this email for your claim: wbuffett4@aim.com (Circumstance) [STX23, CL2.0]

23[You] (Actor) Contact(Material) us (Goal) at this email for your claim: wbuffett4@aim.com(Circumstance)[STX23,CL2.0]

In examples (19, 20, 21, 22 and 23) displayed above the participant 'you' was not explicitly stated in the text but it was rather implied. The scammers gave instructions to the recipients to carryout but the clauses did not explicitly mention the participant 'you'. 'You' was implied and one can infer from the text that the participant 'you' is the recipient since the messages are sent to the recipients.

The agents associated with the material process are mostly male persons. Most of the actions were performed by the male persons or affected the male persons. Bernal and Belli (2013) explained that these scam emails are usually signed by either a man or woman but the real gender identity of these scammers remains a mystery. This means that even though, the male persons dominated as the Actor in terms of the pronoun, it cannot be generalized that the scammers are mostly males. In the analysis, 'he' was used as Actor performing actions in the material clauses more than 'she'. This gives clear evidence of skewed gender in scam email messages. In this study, male persons are either *the victims of a plane crash, in trouble and want the help of the recipients to be liberated or have won lottery prizes and discovered a dormant account.* In Holt and Grave's (2007) study, they noticed that the scammers usually introduce themselves as a male who is either a lawyer, an attorney of a client or a bank manager. This, however, cannot be a basis to associate scamming with male persons only since female scammers can hide behind a masculine identity in as much as male recipients can hide behind the identity of female identity.

Furthermore, the scammers create a fictitious participant, "we", to help them achieve their manipulative purpose. The personal pronoun 'we' was also predominantly used in scam email messages. The scammers used 'we' to show their institutional or organisational identity. The scammers usually gave the impression that they were part

of a reputable institution. The scammers want the recipients to believe in them as they work with a reputable institution. Bano and Shakir (2015) believe that the personal pronoun 'we' evokes familiarity and friendship. This could apply in scam emails as scammers try to make the text appear friendly, so as to win the trust of the recipient and put away fears. The scammers create an impression that they are harmless people and for that reason, they refer to themselves and the institution they work for using 'we' as reference. Sometimes, the scammers also refer to the group they belong to using the plural marker 'we' as seen in example (23, 24, 25, 26, 27, 28 and 29) below. This puts the recipients at ease and clear doubts. The examples below explain this point further.

23. We (Actor) got mugged (Material) last night at gun point (Circumstance) [STX02, CL3.0]. I (Actor)'ll refund (Material) it (Goal) back to you (Circumstance) as soon as we arrive back home (Circumstance) [STX02, CL3.0].

24. We (Actor) will handle (Material) the logistics involved in the movement of the funds to you (Goal) [STX27, CL14]

25. We (Actor) are contacting (Material) you (Goal) now (Circumstance) [STX07, CL10]

26. We (Actor) will suspend (Material) all your pending transfers (Circumstance) [STX07, CL12]

27. We (Actor) are looking (Material) for employees working remotely (Circumstance)

[STX12, CL1.0]

28. We (Actor) can finance (Material) by making investment in form of a debt financing (Circumstance) [STX14, CL5.0]

29. We (Actor) are giving (Material) you (Receiver) a $50 CVS gift card (Goal) for a short time (Circumstance) [STX17,CL1.0]

In example (23) above, the scammer portrays himself as someone who is stranded at an airport with his family. The scammer wants the recipient to believe he is not alone but in the company of his family and needs help not for himself alone but also for the

family. As also illustrated in example (24) above, the scammers portray themselves as working with a group of people. In example (25), the scammers indicate that, the recipient is being contacted by a group, not an individual. They do this to make the recipients believe that they are working for a credible corporation, thereby adding credibility to their claim. In examples (26), the scammer portrays himself as someone working in a financial institution. Example (27) shows the scammers are trying to offer employment to the recipient. Example (28) comes as a company in need of people to undertake a project with in the recipient's home country. Example (29) gives the recipient an offer for a limited period of time. The Actors performing actions in the examples are 'we'. This could help them win the trust of the recipients because, this puts the recipients at ease and clears their doubts about the identity of the sender of the messages.

The findings of Toma and Hancock (2012), Hancock et al. (2008), DePaulo et a.l (2003) and Newman et al. (2003) show that liars tend to use more third person pronouns in order to distance themselves from the lies. The present study challenges this argument as the scammers use more self-oriented references plus an action verb. This means that in scam emails, the scammers identify themselves with the lies and even show commitment as well. The frequent use of the self-reference pronoun means that the scammers play a central role in scam email messages.

The analysis also shows that all the email messages used for this study did not contain names of the recipients. The recipients were addressed with pronouns such as 'you' and 'your'. This could mean that because the scammers send the messages in bulk to different recipients at the same time, it was difficult for them to check the details of the recipients. Examples are illustrated below.

30. I (Actor) saw (Material) your name (Goal) [STX04, CL5.0]

31. Your email (Carrier) appeared (Relational) among the list of beneficiaries (Attribute) [STX07, CL6.0]

32. Permit (Material) me (Receiver) to inform you of my desire of going into business / family relationship with you (Circumstance) [STX03, CL1.0]

In the examples illustrated above (30, 31 and 32), the scammers used either the pronoun 'your' or 'you'. In example (30), the scammers employed 'your' to replace the name of the recipient which is unknown to them. Example (31) employed the pronoun 'your' as carrier. The scammers used these pronouns to replace the name of the recipients which they do not know. This assertion is supported by Behnam, Azabdaftari and Hosseini (2011) who found in their study on discourse of online deception that none of the spam emails they analysed made reference to the name of the recipient or gave the correct address of the recipient. Pronouns were most dominantly used. Some of the email samples for this study were sent by more than one person which meant that the emails were truly sent in bulk to different recipients at the same time. Behnam, Azabdaftari and Hosseini (2011)confirm that the spam emails are also sent in bulk to different users at the time.

The analyses of the material clauses reveal that most of the actions in the text are directed towards a certain goal. The goals are both human and non-human. The goals in the scam emails are mostly directed towards a human, that is, either the scammers themselves or the recipients. The scammers are usually Goals in instances where some duties are delegated to the recipients, while the recipients are mostly the Goals when the scammers are Actors in the material clauses. This shows that whatever actions the recipients take affect the scammers. The scammers also take actions that

affect the recipients. This gives the impression that the main aim of the scammer is to gain access to vital information from the recipients. Examples are illustrated below to explain this point.

32. I (Actor) shall compensate (Material) you (Goal) with an attractive percent of the total funds for your roles/efforts (Circumstance) [STX20, CL3.0]

33. I (Actor) will guide (Material) you (Goal) without any risk involve (Circumstance) [STX4, CL6.2]

34. I (Actor) will furnish (Material) you (Goal) with more information on this business transaction (Circumstance) [STX21, CL11.1]

35. I (Actor) selected (Material) you (Goal) to receive a cash sum of $1.500,000,00 USD (Circumstance) [STX23,CL3.5]

36. We (Actor) are giving (Material) you (Receiver) a $50 Costco gift card (Goal) [STX19, CL1.0]

In examples (32, 33, 34, 35 and 36), it was observed that whatever action the scammers undertake mostly affects the recipients and whatever actions the scammers direct the recipients to undertake affects the scammers. Even in instance where the scammers employed the plural participant 'we', the actions of the group or organization still affected the recipient.

The finding in this study supports Hauch, Blandón-Gitlin, Masip, & Sporer's (2014) findings that liars use more self-reference pronouns when narrating a personal event or an experience where one is personally involved. They further explain that it is difficult for liars to distance themselves from a story where the liars themselves are the main agents since the scammers will have to give their personal experience in those accounts. The scam emails anlaysed for this study were also in narrative form. The stories were basically about the personal experience of the scammers. For this

reason, the scam email messages contained more personal pronouns which made reference to the scammers themselves.

In sum, the material clauses revealed that the scammers portray themselves as negotiable, generous and valuable. The scammers are also seen as the major actors in scam email messages performing the salient actions in the emails. The scammers give justification why they send the scam emails to the recipients without any prior relationship. The scammers also delegate duties to the recipients in the scam emails. The scam emails did not contain names of the recipients. The material clauses also portrayed bias in gender as most of the texts made reference to the male person. The analysis further portrayed the use of 'that' before the Actor to place emphasis on the Actor. There were also instances where 'that' was used as an Actor in the material process for the reinforcement of statements already made in the text.

4.2.2 Relational Process Types

The relational process type is the second most frequent process type in scam email messages. The relational process type contains three main sub-categories. They include the intensive relational process, the circumstantial relational processes and the possessive relational process. This analysis discusses the transitivity pattern of each of the sub-category of relational process and how each reveals the manipulative purpose of scamming below.

4.2.2.1 Intensive Relational Process Type

The analysis revealed that, of the three sub types of the relational processes, intensive relational clauses were mostly employed in scam email messages, followed by the circumstantial, and the possessive was the least in relational process type. The analysis of the scam email messages revealed that the intensive relational clauses

were basically for introducing the scammers' identity and stating their social status in society. The transitivity elements associated with the intensive attributive relational processes reveal the identity of the scammers as credible and respectable persons in society. Let us consider the examples below

37. I (Identified) am (Relational) Mr Abraham Nuru, Accountant by profession,(Identifier) [STX05, CL2.0].

38. I (Identified) am (Relational) Mr. Andrew Edwards, Head of Client Asset Management of my bank (Identifier) [STXO6, CL1.0].

39. I (Identified) am (Relational) Susan Searle, the manager of auditing and accounting department of AFRICA BANK (AB) here in Ouagadougou Burkina Faso (Identifier) [STX21, CL2.0].

40. I (Identified) am (Relational) Dr. Hassan Musa, senior staff of the Nigerian Ports Authority (Identifier) [STX37, CL1.0].

41. I (Identified) am (Relational) (Mrs.) Madeline Howard a widow to late Wright Howard (Identifier) [STX38, CL2.0].

In the analysis, it can be argued that the scammers use the 'I' as the Identified participant plus relational processes with an Identifier participant in the intensive identifying process to introduce themselves, that is, their personal identity, as well as their social identity. The Identifier positions are usually occupied by titles, names and social role or occupational position. The Identified participants are usually realised by personal pronouns. The pronouns basically refer to the scammers themselves, where 'I' is employed as the Identified in the clauses. The pronoun may also refer to the scammers together with their organization or institution where 'we' is employed as the Identified in the clauses. The scammers usually introduce themselves first, give their social identity and even go further to tell their social status in the society. In examples (37, 38, 39, 40 and 41), the scammers first identify themselves with the pronoun 'I' followed by a relational process, which shows the scammer's, state of

being and finally an Identifier which defines the scammers. In the examples (37, 38, 39, 40 and 41) the scammers give their personal identity first, that is, their names before their social status. Their social identities add more information to their identity and hence boost their credibility. This presents the scammers as credible beings. For instance in example (37), after the scammer identified his name as '*Mr Abraham Nuru'* he went ahead to declare his social status as '*Accountant by profession'*, which is the Identifier. The Identifier gives credibility to the scammers. It is also seen in example (38) where the scammer identified himself as *'Head of Client Asset Management of my bank'* which is a very attractive position in his organization. Other attractive positions were given by the scammers as social status in society. In example (39) the scammer gave his status as '*the manager of auditing and accounting department of AFRICA BANK (AB)'* and example (40) as *'senior staff of the Nigerian Ports Authority'*.

The interesting thing to note about examples 39 and 40 is that the scammers mention reputable organizations which are recognized in society. They even go on to mention the name of the country so that the recipients would believe them. They want to clear any doubt about their social status, and that is why they use the names of recognised organizations.

The scammers are mostly aware that a person's status in society is a key consideration for business transaction. This point is supported by Blommaert and Omoniyi's (2006) study of scam emails, where they notice that scammers know that personal and social identity are important consideration in society for one to be considered credible for any proposition. For this reason, the scammers immediately reveal their social status after they reveal their personal identity to the recipient. After the introduction, the

scammers then proceed to the main issues they want to discuss or the reasons why they send the message.

Since the main intention of the scammers is to dupe the recipients, the scammers usually give their social image as someone working in a financial institution, a barrister or a lawyer to a dead client, someone working with a prestigious institution or working under an influential person, to lure the recipients their deceptive narratives. The social status gives the target recipients an impression that they are dealing with a genuine person. Hiß (2015) points out that scammers claim titles for themselves. For instance, the scammer, in example (43), poses as a person with high profile. Since there is no relation between the scammer and the recipient, the scammer has to gain the trust and confidence of the recipient and one way of gaining that trust and confidence is to pose as an influential person in society. The institutions mentioned by these scammers are usually recognizable and respectable institutions in society. They do this to clear any doubt in the mind of the recipients about their social class or profession in society.

This was also noticed in Tan and David's (2017) study of online dating scam, when it was clear from the extracts that the scammer portrays himself as someone with a stable career. The scammers do this to portray themselves as credible, responsible and respectful persons in the society. They tend to give a good image about themselves so as to have an advantage over the recipients. Chiluwa (2006) suggests that the deceivers usually give a brief introduction of themselves in order to establish business and legal requirements of the senders of the messages. The introductions usually identify the scammers with the lies they want to portray. Edelson (2003) found that scammers pose as prominent public officials who have the capacity of making a transaction realizable. Rich (2015) also suggests that scammers are more likely to

represent themselves as professionals working in an organization. They portray themselves as professionals to gain respect and recognition of the recipients. Professionals also have the chances of gaining business recognitions from the recipients.

In addition to social status, the scammers also reveal their marital status in the scam emails. In intensive relational clauses, the scammers employ the pronoun 'I' as an 'identified' plus a relational process 'am' accompanied by an 'identifier'. The identifiers in this case are usually adjectival phrases. In the text, the adjectival phrases usually contain the name of the Identifier with an adjective which realizes the Attribute assigned to the Identifier. The adjectival phrases add more information about the Carriers. In African culture and in many other parts of the world marriage is very important. It is therefore assumed that married people are matured and respectable. This motivates the scammers to portray themselves as such which is reflected in the examples below. As examples (42) and (46) show, some of these clauses are identifying relational clauses, where the marital status, the attribute, is realized as an appositive to noun group representing the name of the writer.

42.I (Carrier) am (Relational: attributive) married to Mr. Greg Johnson (Attribute) [STX25, CL6.0].

43.I (Carrier) am (Relational: attributive) married to Mr. Mark Mogab (Attribute) [STX26, CL2.0].

44.I (Identified) am (Relational: identifying) (Mrs.) Madeline Howard a widow to late Wright Howard (Identifier) [STX10, CL4.0].

45. I (Identified) am (Relational: identifying) Mrs Torli Benzel a widow from Switzerland based in Ivory Coast (Identified) [STX10, CL4.0].

46. My Name (Identified) is (Relational: identifying) Mrs. Catherine. Thomas (Identifier) [STX11, CL2.1].

As seen in examples (44 and 45,) above, the scammers reveal their marital status to the recipients. Even in examples (47 and 48), the scammers show that they were once married but their husbands are dead. Those scammers who do not state that they are married give their marital titles *"Mrs."* as reflected in example (46) *'Mrs. Catherine. Thomas'* which clears any further questions concerning their marital status. The scammers do that to show how responsible they are, because a married person is seen as responsible and respectable in most societies especially in Africa. This will encourage the recipient to have confidence in the scammers and thereby accede to the deceptive plans.

The study also shows that the introduction the scammers give about themselves either personal or social, usually influences the content of the messages. After the scammers introduce themselves to the recipients, they then proceed to tell their purpose for writing such a mail. This is mainly done through identifying relational clauses. The scammer's introductions usually have a link with the content of the message. The examples below are used to explain this point further.

> 47.I (Identified)'m (Relational) Sgt. Martins George, a U.S. Army now on tour of duty in Kuwait (Identified) [STX01, CL1.0].
>
> 48. I (Identified) am (Relational) Wilson Koh, a native of Iraq (Identifier) [STX08, CL1.0].
>
> 49. My name (Identified) is (Relational: identifying) Mr. Akinwumi Godson Fanimokun, Group Executive, Technology & Services First Bank of Nigerian Plc. based in Nigeria (Identifier) [STX22, CL1.0].

In the examples (47, 48 and 49), the scammers, after identifying their names give brief introductions of themselves. The brief introduction can also aid the recipients in understanding the content of the message. For instance, in example (48), the scammer reveals that he is a citizen of Iraq, and in the content of that message, the scammer

needed the help of the recipient to move from Iraq because of war. The recipient will then reflect on his knowledge about Iraq which gives the recipient an idea of what the scammer may be going through in Iraq which is a war torn country. Also in example (49), the scammer revealed his identity as working in an organization; the scammer then invited the recipient to invest in their company for profitable interest. From the examples, it was noticed that the scammers' identities had a great influence on the content of the message.

Adegbija (1995), as cited in Chiluwa (2006), says that scammers usually see the introductions as a way of preparing them for a successful interaction. The introductions used by scammers could also give the recipients an idea about the message in the content of the text. Chiluwa (2006) further explains that the introduction clears any suspicions in the minds of the recipients because the scammers are usually unknown to the recipients. When one considers example (48) again, one notices that the scammer wants to relocate to the recipient home country because Iraq is at war . The recipient is likely to understand the scammer because there had been an incidence of war in Iraq.

Moreover, cultural factors influence the introduction given by the scammers because it is common in most cultures to introduce oneself before initiating a conversation. In African culture, greetings and introduction of oneself is very important before any successful interaction. It prepares the way for good interactions.

4.2.2.2 Circumstantial Relational Process

In the analysis, a total of 32 circumstantial relational clauses were identified in scam email messages, representing 13.3% of the clauses analysed. The circumstantial relational processes were used to give additional information about the scammers, the

transaction or their client. This additional information is meant to clarify issues better to the recipients. If the scammers portray themselves as lawyer to a dead client then, there is the need to specify the time the client died and what caused his death. This is done using the circumstantial relational clause. Examples are illustrated and discussed below.

50. Sorry if you received this letter in your spam, it (Carrier) is (Relational: attributive) due to recent connection error here in the country (Attribute: circumstantial) [STX05, CL11.0].

51. He (Carrier) was (Relational: attributive) among the death victims of the May 26, 2006 Earthquake disaster in Jawa, Indonesia(Attribute: circumstantial) [STX06, CL5.1].

52. He (Carrier) was (Relational: attributive) on a business trip in Indonesia during this disaster (Attribute: circumstantial) [STX06, CL6.0].

53. She (Identified) is (Relational: identifying) not here with me any more(Identifier: circumstantial)
[STX23, CL18.5]

54. A lot of people (Identified) are (Relational: identifying) out there (identifying: circumstantial) to discourage them(circumstance) [STX23, CL19.6].

55. This (Identified) is (Relational: identifying) due to the urgency of this project (Identifier: circumstantial) [STX35, CL1.1].

In the examples (51, 52, 53, 54 and 55) above, the scammer provides additional information which is crucial for the success of the transaction. The scammer know some of their messages usually go to spam, so he makes the recipient aware that the message is not spam and if it goes to spam then it an error in network connection as seen in example (50). Examples (51, 52 and 53) specify information about the dead client. Also, the scammer specifies the urgency of the message in example (55), which is why he contacted the recipient. The information provided gives more understanding

about certain issues already mentioned in the text by the scammer. The further clarification will help the recipient to get a clearer image of the whole text.

The analysis of the circumstantial relational clauses also presents the scam email messages as genuine. The scammers use the circumstantial relational clauses to provide additional information which boosts the credibility of the message as illustrated in the examples below.

> 56. I (Carrier) am (Relational: attributive) in desperate need of your assistance to help me receive US$8M in your home (Attribute: circumstantial) [STX01, CL2.0].
>
> 57. I (Carrier) am (Relational) from Kuwait (Attribute: circumstantial) [STX26, CL1]
>
> 58. I (Carrier) have been (Relational: attributive) in search of someone with this same last name (Attribute: circumstantial) [STX06, CL4.0].

In examples (56, 57 and 58) above, the scammers provide information about themselves which relate them to the transaction they want to undertake. For instance, in example (56), the scammer needs the help of the recipients to receive some huge sum of money on his behalf. Example (57) reveals the scammer country so the recipient will reflect on his background knowledge about that country to know what is taking place that prompted the scammer to send such a message. The scammer showed in example (58) that, the name of the recipient motivated him to send such a message. So it relates the scammer to the text very well and portrays him as genuine.

The circumstantial relational clauses are also used to give more information about the transaction and present the attractive package which awaits the recipients in case the transaction is successful. This strategy is used to lure the recipients to act, as the money involved is usually huge. Examples are highlighted below.

59. The check (Carrier) was (Relational: attributive) in the Amount of TWENTY MILLION US DOLLARS (Attribute: circumstantial) [STX39,CL3.0].

60. The funds of this account (Carrier) valued at (Relational: attributive) $85.5 Million usd (Attribute: circumstantial) [STX21, CL7.2].

61. These boxes (Carrier) are (Relational: attributive) in Security Company (Attribute: circumstantial) [STX08, CL6.1].

62. The maturity date for this deposit (Identified) was (Relational: identifying) on 2007 (Identifier: circumstantial) [STX06, CL5.0].

In examples (59, 60, 61 and 62), the scammers displayed the amount of money involved in the transactions. As for example (59), the scammer specifies the amount in uppercase *'TWENTY MILLION US DOLLARS'* so as to draw the recipient's attention to it immediately the email is read. The value of the money is given as *'$85.5 Million usd'* in example (60). We notice in example (59 and 60) that the amounts are stated in dollars and this shows that the money is huge and the recipient will be motivated to reply because of the amount involved. Example (62) specifies the date the money was due for maturity and the recipient can claim this money if he agrees to the propositions in the email he received.

4.2.2.3 Possessive Relational Clauses.

The scammers employ the carrier 'I' plus a relational verb accompanied by a circumstance to reveal the positive qualities they possess. It gives them the opportunity to narrate their stories and bring out their unique qualities. This is one strategy of luring the recipients to believe in the deceptive stories. The possessive relational clauses reveal the kind of wealth or qualities the scammers possess which make them prominent people in the society and these add credibility to the scammers. The possessive relational clauses usually were used in scam email messages after intensive relational clauses.

It is evidential from the intensive relational clauses displayed earlier (examples 34, 35 and 36), that the scammers portray themselves as prominent people in society. Prominent people usually possess some great wealth or have advantages in terms of business transactions in society. Based on this argument, the scammers therefore go ahead to declare their wealth or an important proposal they possess which would be beneficial to the recipients. The scammers also portray themselves as good people and that is why they are contacting the recipients for such a transaction for mutual benefit.

This suggests that though the scammers use a lot of intensive relational clauses to reveal their personal identity and social status, they also use the possessive relational clauses to show what they have, ranging from qualities to material possessions. Examples are illustrated below to highlight this point.

63. I (Carrier: possessor) have (Relational: possessive) a good heart (Possessed) [STX21, CL6.0]

64. I (Carrier: possessor) have (Relational: possessive) all the legal document (Attribute: Possessed) with me (circumstance) [STX21, CL8.1]

65. I (Carrier: possessor) have (Relational: possessive) a proposal (Attribute: possessed) [STX27, CL2.1].

66. I (Carrier: possessor) have (Relational: possessive) a very sensitive and confidential brief (Attribute: Possessed) for you from international bank of Taipei, Taiwan (circumstance) [STX28, CL1.1].

67. I (Carrier: possessor) have (Relational: possessive) US$56,000.000 (fifty Six Million United States Dollars) for investment purpose(Attribute: Possessed). [STX32, CL6.0].

68. I (Carrier: possessor) have (Relational: possessive) a Business worth $47.1M USD (Attribute: Possessed) for you to handle with me (circumstance) [STX36, CL3.0].

70 I (Carrier: possessor) have (Relational: possessive) some funds (Attribute: Possessed) [STX38, CL3.0].

71. I (Carrier: possessor) had (Relationsal: possessive) a client (Attribute: Possessed) [STX40, CL2.4].

In example (63), the scammer identifies the personal unique quality he possesses which is "good heart". This scammer believes his good heart is an essential element for the transaction. So in this example, the scammer employs the Carrier 'I' with a relational verb accompanied by the Attribute he possesses. This also reflects that, in scamming, the personality of a person is considered important. The scammers also reveal the wealth they possess as shown in examples (67 and 68) as *'US$56,000.000 (fifty Six Million United States Dollars'* and *'$47.1M USD'* respectively. The wealth is usually given in huge sums of money. The scammers mention the huge sum of money to lure the recipient into accepting the proposition. The scammers also specify in examples (64) that they have all the necessary documents and arrangement needed for a successful transaction. They assure the recipients that there will be no delay as all the necessary arrangements and documents are available at their disposal.

The scammers also employ the Carrier 'you' plus a relational verb and a possessed Attribute to show the unique qualities that the recipients possess which are vital for the transaction. The examples below reveal the qualities the recipients:.

> 72. You (Carrier: possessor) have (Relational: possessive) this money (Attribute: Possessed) in your personal account (circumstance) [STX23, CL16.4]
>
> 73. You (Carrier: possessor) have (Relational: possessive) the same last name with my late client (Attribute: Possessed) [STX29, CL2.2].
>
> 74. You (Carrier: possessor) have (Relational: possessive) any viable project we can finance by making investment in form of a debt financing (Attribute: Possessed) [STX14, CL4.0].

Examples (72 and 73), above indicate that the target recipients possess a lot of positive attributes which make them qualify to handle the propositions brought before them. However, in example (74), the scammers entreat the recipient to reply if he possesses the attribute mentioned, that is, *"any viable project"*. This suggests that in

scamming, scammers also specify the kind of attribute they expect the target recipients to possess in order to make the proposal a success.

Also, the scammers could identify the qualities their client or organization possess which would be beneficial to the recipient. In cases where the recipients are dealing with other clients, the qualities the clients possess are made known to the recipient.

> 75. My Client (Carrier: possessor) had (Relational: possessive) businesses (Attribute: Possessed) in Ghana and the Middle East (circumstance) [STX40, CL2.4].
> 76. She (Carrier: possessor) has (Relational: possessive) a huge amount of money in the excess of (25, 000,000) pounds twenty five millions pounds (circumstance) [STX30, CL3.0].

In examples 75 and 76, the scammers revealed the amount of wealth their client possess to the recipients. Example 75 went ahead to specify the countries where the client had the business.

Again, the meaning patterns of the possessive relational clauses show the recipients as significant figures in the transaction. The recipients are usually portrayed as people who possess a feature worthy of making the transaction possible.

In sum, the analyses of the relational clauses reveal the following interesting findings which are summarised below.

First, the intensive relational process types are used by scammers to introduce themselves, state their social status so as to be considered as genuine and credible. The scammers give their personal identity and social status in society, as well as, show their level of importance in the society.

Then, the circumstantial relational process type is used to give additional information about the transaction so as to clear any misunderstanding or doubts in the mind of the recipients. It is also used more to specify issues in the text to the recipients.

Also, the possessive relational process types are used to highlight the qualities that the scammers or their organizations/ institutions possess which would be beneficial to the recipients as well as showcase the qualities the recipients possess which are beneficial for the success of the transaction.

4.2.3 Mental Processes

The mental clauses demonstrate the feigned commitment and dedication of the scammers towards the scammed transactions. There were various Sensers employed in the scam email messages. The most often employed sensors were the personal pronouns. Most of the mental activities were initiated by the scammers. Examples from the text are illustrated below to explain this point.

> 77. As the director of the department (Circumstance), this discovery (Goal) was brought (Material) to my office (Circumstance) || so as to decide (Mental) what is to be done (Phenomenon). I (Senser) decided (Mental) to seek ways through which to transfer this money out of the bank and out of the country too (Phenomenon). [STX01,CL3.0]
>
> 78. I (Senser) decided (Mental) not to remarry or get a child outside my matrimonial home(Phenomenon) <<which the Bible (Carrier) is (Relational: attributive) against (Attribite)>> since his death (circumstance). [STX28, CL2.1]
>
> 79. I (Senser) decided (Mental) to relocate to your country (Phenomenon). I (Carrier: possessor) got (Relational: possessive) your contacts (Attribute: Possessed) through my personal research and out of desperation (circumstance). I (Senser) decided (Mental) to reach you through this medium (Phenomenon). [STX34, CL3.0]

The scammers feigned commitment and dedication because most of the psychological decisions were initiated by the scammers themselves. In examples 77, 78 and 79 above, it is observed that the scammers denied themselves of certain privileges in order to make the content of the message fulfilled. The scammers portray themselves as people who had the opportunity to do other things but decided to forgo them as in example 77 and 78, which indicate their commitment and dedication. The scammer had the opportunity to decide what to do with the money in example 77, so he decided to consult the recipient for their mutual benefits. Also in example 78, the scammer had the opportunity to marry but decided to keep to her matrimonial vows. These show their commitment and dedication towards the message. The recipients would, other things being equal, therefore, have no reason not to believe these lies and also challenges the recipients to show commitment and dedication just as the scammers did. The recipients may also have to sacrifice something to make the wish of the scammers come true. The recipients are made to believe that they would benefit from whatever commitment and dedication they make towards the success of the transactions.

Another interesting thing about the Sensers is the sub-type of mental processes associated with them. The sub-type associated with Sensers in scam emails messages were cognition, desideration, emotion and perception. However, desideration was predominantly used in the scam email messages. Table 4.2 shows the types of mental processes used in the scam email messages and their frequency distribution.

Table 4.2: Distribution of Mental Clauses across the Sub-Types of Mental Processes

Mental Process type	Frequency	Percentage (%)
Desiderative	61	48.03
Cognitive	48	37.03
Perceptive	10	7.80
Emotion	8	6.30
Total	**127**	**100**

In Table 4.2 displayed above, the frequency of occurrence of the sub-types of mental process and their frequency are illustrated. The desiderative mental process type was dominantly used in the scam email messages analysed with a frequency of 61, representing 48.03% of the clauses analysed on the mental process types. The cognitive process type was the second frequent mental process type, with a frequency of 48 and a percentage of 37.03%. The least frequent mental process type was the perceptive and emotive, with a frequency of 10 (ie.7.80%) and 8 (6.30%) respectively.

This reveals that, in scam email messages, the scammers have a desire which they want the recipients to help them fulfill. They therefore have to manipulate the recipients using lies in order for him or her to agree to their selfish and greedy desires. Rich (2015) said that scam messages appeal to trust and greed. The greedy nature is portrayed when the scammers attempt to dupe people millions of money and properties. The desiderative verbs, such as *'decided', 'want',* and *'wish'* were frequent in the scam email messages. This reveals that utmost important to scammers is fulfillment of their desires. The following examples clarify the point.

80. I (Senser) need (Mental) your help(Phenomenon) to fulfil my last wish (circumstance).[STX10,CL3.0]

82. I (Senser) will like (Mental) us to keep via email for now (Phenomenon).[STX06.CL14]

83. I (Senser) want (Mental) you to take 15% of the total $3,000,000.00 (Phenomenon) for your efforts (circumstance).[STX10,CL7.0]

In examples, 80, 81,82, and 83, the scammers employed the Senser 'I' plus mental verbs *'decided', 'need', 'like', 'want'* and *'wish'* in the mental clauses. The sub-type associated with the mental verbs in these examples (80, 81, 82 and 83) is desiderative. In example 82, the scammer wants the help of the recipient to fulfill his last wish. It can be deduced from the clause that the fulfillment of the wish is a desire and the main aim of the scammer is to achieve it. Example 83 also follows the same purpose; the scammer wants the recipients to do something for him.

Scammers constantly come out as persons that have much control of their mental processes. The cognitive sub-type was the second predominantly used sub-type associated with the Senser 'I'. The scammers employ the Senser 'I' plus a cognitive verb accompanied by a phenomenon to show their cognitive capacity. The scammers are usually the ultimate decision makers in scam emails. The scammers are aware of the consequences of their actions, so they do the thinking as illustrated in examples 81 and 81 below, while the recipients are usually presented with choices. The recipients are usually motivated by the scammers to fulfill those choices in return for some rewards.

The scammers do not give the recipients the opportunity to do much thinking as reflected in the texts, because any wrong actions they take will either affect or make them. The examples below explain this point.

84. I (Senser) hope (Mental) this information meet you well (Phenomenon) [STX 23, CL3.0].

85. I (Senser) know (Mental) you will be curious to know why/how (Phenomenon) [STX23, CL 3.1].

86. I (Senser) don't know (Mental) when I will die (Phenomenon) [STX23, CL12.3].

87. I (Senser) am hoping (Mental) you will be able to use the money wisely and judiciously (Phenomenon) over there in your country (Circumstance) [STX23, CL15].

88. I (Senser) know (Mental) where I'm going (Phenomenon) [STX26, CL16.1].

In examples 84, 85, 86, 87 and 88, the scammers employ the senser 'I' plus a cognitive verb such as *'hope'* and *'know'* accompanied by a phenomenon to demonstrate the thinking they do before presenting the proposal to the recipients. The examples illustrate that the scammers do the thinking and then present the choices to the recipients. The scammers do not allow the recipients to do the thinking but they are allowed to after all the options are considered and presented before them.

The recipients are usually asked to get further clarification from the scammers when something is not clear. The scammers usually make provision for the recipients to seek for clarification in order to get a better understanding of the text. This clears any misunderstanding the scammers have in their mind. The scammers direct the recipients either to a website or provide details in the text. Sometimes, the scammers ask the recipients to contact them directly through a provided address. All that the scammers want is for the recipients to understand the email messages better and make a choice which will favour the success of the deceptive proposals. Examples are provided below.

89. You (Sensor) can see (Mental) more information about Saba Masri Mr.Moises unfortunate end accident (Phenomenon) on the website-link below (circumstance) [STX21,CL4.0].

90. You (Sensor) see (Mental) the link below (Phenomeon) [STX22,CL3.8]

91. you (Sensor) could see (Mental) from the webpage above (circumstance) [STX23,CL8.0]

In examples 89, 90, and 91, above, the scammers employ the Senser 'you' plus a perceptive mental verb *'can see', 'see'* and *'could see'* and a phenomenon which specify where the recipients can get more clarification about the deal. These verbs give the recipients explicit information as the information the scammers want the recipients to see are normally provided in the text. In the example 89, the scammers provide the recipient with a website where more clarification about the transaction will be given. The scammers do not allow the recipient to think through the propositions presented before them. They expect the recipients to get all the clarification from them. That is why in example 91, a link is provided where the recipient can seek more clarification when in doubt. Example 89 is different, as the scammers provide the details in the text itself. The scammers provide all the information needed by the recipients to understand issues in the text. When we consider all the examples 89 to 91 above, we notice that the scammers do not tell the recipients to think through the messages and make a choice. They rather provide them with directives as to where to gain more clarification and decide whether to take up the transaction or not. However, the recipients are usually encouraged to agree to the proposals.

The transitivity patterns identified in the mental process types are summarized below. First, the mental process type portrays the scammers as committed and dedicated to the success of the transactions.

Second, the mental process types show that the scammers employ more desiderative verbs in their narratives thus, revealing their greedy and selfish nature.

Third, the scammers also do most of the thinking and leave the recipients with choices to choose from only. The scammers also use perceptive verbs to give the recipients additional information concerning the transaction, they also provide the recipients with addresses to contact for further clarifications when in doubt about anything concerning the propositions.

4.2.4 Verbal Process

The transitivity patterns in which the scammers are the Sayers highlight three interesting issues. The patterns show that the Sayers in verbal processes are usually thanking the recipients, apologising, and seeking for assistance from the recipients. Forty-four verbal processes were identified in the analyses representing 5.1% of the clauses. Let us consider the examples below:

92. Thank (Verbal) you (Receiver) very much for your urgent response to me (circumstance: Matter) [STX21, CL1.0].

93. Thank (Verbal) you (Receiver) for accepting our offer (circumstance: Matter) [STX23, CL20.0].

94. Thank (Verbal) you(Receiver) for your cooperation (circumstance: Matter)[STX13,CL9.0]

Regarding example 92, the scammer thanks the recipient for response which is yet to be given. The same applies to example 93 where the scammer thanks the recipient for accepting the offer, though, the scammer is yet to give feedback from the recipient. This is a strategic element used to gain response from the recipients. It is also meant to induce the recipient to response to the messages.

The scammers use the verbal process ‘thank’ with a Receiver ‘you’ accompanied by the circumstance of the Matter to express their gratitude to the recipients. The two examples displayed above do not contain any explicit Sayers. The Sayers in the two

examples are implied, who are basically the scammers. The scammers show their appreciation before the recipients even accept the offer they are trying to negotiate. This shows that in scam email messages, scammers try to show appreciation and gratitude to the recipients even though they are not certain whether the negotiation between the two parties (which is the scammers and the recipient) will succeed. They do this so the recipients may feel sorry to turn them down since they have already raised their hopes

Also, the scammers employ the Sayer 'I' plus a saying verbs accompanied by Matter to apologize to the recipients. The scammers are much aware that the method they use to send scam email messages is not appropriate. They therefore apologize to the scammers before proceeding to give the message to the recipients. This will help calm the recipients nerves and prompt them to read the content of the message. In example 95 illustrated below, we notice that the scammer apologize for *"sending you this sensitive information via e-mail instead of a Certified Post-mail"* and also apologize in example 96 *"if the contents in this mail are contrary to your moral ethics"*. This means that scammers know the medium they use to write the message is dubious but they apologise to cover up their dubious plans. We also notice in example 97 that after the scammers apologise, they go on to tell the recipients the duties they would play to make the proposition a success.

95. I (Sayer) apologize (Verbal) for sending you this sensitive information via e-mail instead of a Certified Post-mail(circumstance) this(Identified) is(relational: identifying) due to the urgency of this project(Identifier: circumstantial). I (Sayer) will introduce (verbal) myself (Target) to you [first] (circumstance: Matter) [STX, CL1.0].

96. I (Sayer) apologize (Verbal) || if the contents in this mail (Carrier) are (Relational: attributive) contrary to your moral ethics (Attribute) [STX25, CL1.0].

97. I (Sayer) will instruct (Verbal) the Bank Manager (Receiver) to issue you an authority letter [[that will prove you the present beneficiary of the money in the bank]] (Verbiage)

Also, the pattern reveals the religious bias of the scammers. They use "God" as a Sayer three times in the verbal processes. This is to appeal to the religious feeling of the recipient. The scammers use religion to influence the recipients to see them as God-fearing and holy. The religious comments usually appear at the closing of the scam email messages. This is a form of evoking the emotions of the recipients to respond. It was noticed that some made reference to the Bible while others made reference to the Quran. The scammers believe making religious comments may appeal to the emotions of the recipients and lure them to respond to the message. This shows the influence of religion on some email scammers. Chiluwu (2006) also noticed in her study that deceivers tended to use religion to influence recipients because they had much knowledge about how religion was influencing the way of life of people in the world. There were instances when the scammers quoted the Bible to defend their point. Example 98 below shows an instance where the scammer quoted the Bible to make a point and to appeal to the religious emotions of the recipient.

98. Exodus 14 vs 14 (Sayer) says (Verbal) || that the lord (Actor) will fight (Material) my case (Scope) [STX26, CL18.0].

This example (98) was placed inside rescue operation category of scam email messages. The scammer portrayed himself as someone who needs help to move out of his country to the country of the recipient due to a threat on his life by some business partners of his late father. He therefore needs the help of the recipient. The scammer used this quote from the Bible to show his religious nature and also appeal to the religious feeling of the recipient.

Holt and Grave (2007) also note that the scammers make reference to fasting and prayers in the scam email messages to show their Christian nature and also portray themselves as born again Christians, God fearing and prayerful. Some of the headings of the messages, especially those which belong to charity category started with religious greetings. The scammers were aware of the impact of religion on a recipients's life. Therefore religion can also be used to influence the recipients to respond to their deceptive messages.

4.2.5 Behavioural Process

The behavioural clauses contained only one unique pattern, which is, urging the recipients to act immediately. In the analysis, three behavioural process types were identified in three different scam emails. But, interestingly, the same process type was repeated three times in three different scam email messages.

99. [You] (Behaver) Do not wait (Behavioural) [STX17, CL5.0].

100.[You] (Behaver) Do not wait (Behavioural) (STX18, CL5.0]

101. [You] (Behaver) Do not wait (Behavioural) [STX19, CL6.0)

These were the behavioural processes repeated in three scam email (STX17, CL5.0, STX18, CL5.0, STX19, and CL6.0]

In the analysis, there was an implied 'you' which refers to the recipients and a behavioural verb. This behavioural clause occurred at the concluding part of the scam email messages. This gives the impression that the scammers used this process to stimulate the fastness of the recipients to the messages. The behavioural process appeared in the form of exhortation in the scam email messages. As the scammers want to portray that any delay could cause the recipients to lose something valuable.

4.2.6 Existential Process

Table 4.3 Samples of Existential Clauses in Scam Emails

Text no	Dummy Subject	Process	Existent	Circumstance
STX06, CL11.2	There	is	No risk involved	
STX13, CL5.1	There	is	a possibility	of gaining the money
STX10, CL3.0	There	is	the sum of $150,000,000.00	in my bank

In the analysis, only three existential processes were identified and they were all connected with the transaction. The scammers employ a dummy subject 'there' plus a process 'is' and an Existent accompanied by a circumstance. The circumstances give additional information but do not have any effect on the clauses. The scammers want to let the recipients know that the transaction is not harmful or will not cause any damage to the recipient as illustrated in (STX06, CL11.2). This finding is in line with Holt and Grave (2007), Edelson, (2003) study of scam emails, this strategy could motivate the recipient because they do not stand to lose anything in case things go wrong. Moreover, the transaction is risky to their life

In (STX13, CL5.1), the scammer wants the recipient to know that the transaction is possible and he could gain much if it succeeds. The scammers also specify the amount that exists in the transaction in (STX10, CL3.0). The amount is meant to influence the recipient because it is a huge sum of money. Since the recipient does not lose anything in this transaction and the amount involved is huge, he may be tempted to give it a try. The circumstances associated with the existential process make reference to money and a financial institution. This shows how far the scammers go in order to succeed in getting the recipients to respond to their deceptive messages.

4.3 Summary of the Chapter

This chapter has discussed the process types used by scammers to manipulate recipients of scam email messages. It has also discussed the transitivity patterns employed in scam email messages and how they reveal the manipulative purpose of scamming.

The first section of the analysis revealed that scam emails contain more material, relational and mental process types than the verbal, behavioural and existential. This means that scamming is basically associated with actions and happening, sensing and having-&-being than the other domains of experience.

The second section discussed the transitivity patterns used in scam emails. The findings are summarized below.

First, the transitivity patterns of the material process type revealed that scammers portray themselves as generous, negotiable and valuable.

Second, the transitivity pattern of the mental processes indicate that the scammers feigned dedication and commitment towards the scammed transaction.

Third, the transitivity pattern of the relational processes revealed that scammers portray the positive qualities they possess and also the qualities that the recipients possessed.

Fourth, the transitivity patterns of the verbal process type project the scammers as grateful beings who thank the recipients even before receiving feedback and present them as religious.

Firth, the transitivity pattern of the behavioural process was presented in the form of exhortation, that is, urging the recipient to act immediately.

Finally, the transitivity pattern of the existential processes was presented in the form of a motivation which was basically to assure the recipients that no risk are involved in the transactions.

Thus transitivity patterns of the six process types, which are, the material, relational, mental, verbal, behavioural and existential, revealed that the manner in which personal pronouns were used in scam emails demonstrated two interesting interpersonal orientations: the 'I'-orientation, where the 'I' is thematised as subject of a clause and the 'you'-orientation, where the 'you' is also thematised as the subject of a clause.

CHAPTER FIVE

CONCLUSION

5.0 Introduction

This final chapter summarizes the major aspects in the research. The chapter also presents some recommendations for future research. These are followed by summary of the research finding and finally some concluding remarks.

5.1 Summary of Aims and Methods

The main aim of the study was to investigate how deception is enacted in scam email messages. The study addressed two important issues. Firstly, it examined the process types used for manipulating recipients of scam emails. Secondly, it explored the transitivity patterns (i.e. verb choices and participant roles involved) used in scam email messages by the email scammers to construe fraud in an attempt to manage information in order to manipulate email recipients and how they reveal thus reveal manipulative purpose of scamming.

In light of this, the study employed two concepts in Halliday's Systemic Functional Linguistics that is, the 'systemic network' and the 'metafunction' which served as a guide to achieve the aim of this study. The systemic network shows that speakers of a language have choices when speaking or writing. The idea of metafunctions also shows that language performs three major functions. The three functions are the ideational, interpersonal and textual metafunction. The ideational function represents the experiences of people. The interpersonal function is the use of language in negotiating meaning in interaction. The textual function relates the experiences of an individual to a text. The ideational was applied in this study. The study used the ideational metafunction as a guide to carry out this study. The study revealed how

scammers present their experiences of both the physical and mental world through the use of language. Transitivity was the main analytical framework used in the analysis of this study.

The study employed the qualitative research approach because the study was descriptive in nature. The qualitative research approach allowed the researcher to describe concepts employed in the analysis of the data for this study. Also, Burton's method of analyzing was employed to analyze and interpret the data. Burton's method of analyzing helps to isolate the process in each clause and identify the participants, as well as the role each participants plays in the text. The study therefore employed this method to identify the various process types (ie material, mental, relational, verbal, behavioural and existential) in scam email messages and the participants associated with those process types.

The study addressed the first research question which is (What process type(s) is/ are used for manipulating recipients of scam emails?) by chunking the clauses and identifying the process types in each clause. The process types were then counted and the dominant process type which occurred in the text recorded. Quantitative techniques were employed in this section to answer research question one. The study employed frequency count and percentage distribution of the six process types in this section. The frequency of occurrence of the six process types (ie. material, relational, mental, verbal, behavioural and existential) was recorded and the percentage distribution of each also calculated. These were displayed in order of the frequency of occurrences.

With regard to research question two, (What transitivity pattern(s) is/are used to manipulate recipients of scam emails and how do they reveal the manipulative

purpose of scamming?), after sorting and identifying the process types, the participants employed in each process types were identified. The functions these participants played were highlighted. The circumstances associated with the various process types were also analysed. The repetitive patterns in each process type were identified. The patterns in which those repetitions occurred in each process type were also analysed. After identifying and analyzing repetitive patterns, the study demonstrated how the patterns analysed in each process type revealed the manipulative purpose of scamming.

5.2 Key Findings

The study noted some key findings with regard to the two research questions posed in chapter one. First, in relation to the process used by scammers to manipulate recipients of scam email messages, the study showed that material, relational, mental, verbal, behavioural and existential processes were employed in scam email messages. The highest percentage (51.4) was the material, which dominates the entire process in the scam email messages. The relational was the next dominant process type with percentage of (28.0%), followed by the mental with a percentage of (14.7%). The mental process had sub types which occurred in scam emails as illustrated; desiderative: 61 times (ie.48.03%), cognitive: 48 times (ie.37.80%), perceptive: 10 times (ie.7.87%) and last, the emotive: 8 times (ie.6.30%). The verbal process followed with a frequency of (5.1%). The least occurring were the behavioural and existential with a percentage of (0.4%) respectively.

The scam email messages were dominated by the material, because scamming is mostly associated with material process, which is, performing certain actions and indulging others to perform certain functions as well. The relational also illustrates

that scammers identify the relationship between themselves and their recipients before proceeding on their deceptive acts.

The findings also revealed that the scammers employed certain types of verbs more frequently in each of the process types. The process type which occurred most had certain verbs frequently used. The material process had the verb 'write' appearing more frequently. The relational process type had the linking verbs 'is, was, were' appearing more than any other verb. The mental process type had the desiderative verb 'want' appearing more than any other verb.

The second key findings were in relation to the transitivity patterns (i.e. participant configuration, specific verb choices for processes, circumstantial elements) used to manipulate recipients of scam emails. The transitivity patterns identified in each of the process type and how they reveal the manipulative purpose of scamming are stated below.

The transitivity patterns of the material processes in scam email messages show that the scammers variously position themselves as negotiable, vulnerable and generous. It was also observed that in scamming, scammers do not impose decisions or proposals on recipients. They rather present their message in the form of a preposition which the recipients are not obliged to respond to immediately, which presents the scammers as negotiable. The finding also demonstrated that the scammers provide justification for their actions in the material clauses, which portrays them as generous. The scammers also portray themselves as vulnerable and the recipients will have to rescue them by responding to the email messages. The scammers also portray themselves as generous by stating their intentions regarding how the transaction will take place. The material clauses reveal the imposition of responsibilities on the recipients by the scammers.

The findings also revealed that the agents associated with the material process are mostly male figure. The scammers create a fictitious participant "we" to help them achieve their manipulative purpose in the material clause. The use of self-oriented reference was also dominant in the material clauses.

The transitivity patterns associated with the intensive attributive relational processes reveal the identity of the scammers as credible and respectable persons in society. The intensive relational clauses were basically for introducing the scammers' identity and stating their social status in society. The scammers also revealed their marital status in the scam emails. The analysis of the circumstantial relational clauses present the scam email messages as genuine. The circumstantial relational processes were used to give additional information which buttress earlier information provided by the scammers about themselves, the transaction or their client. The additional information then give the recipients more insight about the transaction. The analysis of the patterns of the possessive relational clauses portrays the recipients as significant figures in the transaction. The scammers revealed in the possessive relational clauses the unique qualities the recipients possessed which was crucial for the transaction. The scammers also justified the qualities their client or organizations possess which would be beneficial to the recipients in the possessive clauses.

The mental clauses demonstrate that scammers feigned commitment and dedication towards the scammed transactions. The mental process types also demonstrate that the scammers employ more desiderative verbs which reveal their greedy nature. The mental clauses also portray the scammers as people who have much control of their cognitive ability. The mental processes further show that scammers provide recipients with extra information about the transactions by directing them to websites or provide them with institutional or personal email addresses.

The pattern of the verbal process type shows that the Sayers in verbal processes are usually thanking the recipients, apologizing, and seeking for assistance from the recipients. The finding revealed that scammers try to show appreciation and gratitude to the recipients before they even get a response from the recipients. The pattern of the verbal process also reveals the religious nature of the scammers.

The behavioural clauses were presented in the form of exhortation which urged the recipients to act without delay, in order not to lose an offer.

The existential clauses demonstrated the existence of huge sums of money. This was meant to motivate the recipients to act upon the scam email messages.

5.3 Conclusions

The following conclusions were drawn from the work with regard to the research questions posed in chapter. First, the study confirmed that the frequency distribution of clauses across process types in the scam email messages is not marked when we compare it to the typical distribution of process types in English discourse. The scammers used the material, relational, mental, verbal, behavioural process types in scam emails, which is mostly same in most English discourse(Martin 2016; Halliday and Mathiessen 2014; Matthiessen 2007: 812). Also, it was noticed that scam emails involve more of actions and happenings, sensing and having-&-being than saying, behaving and existing.

Secondly, the study demonstrated that scammers portray themselves as generous, negotiable and valuable in the material clauses, the mental clauses revealed that the scammers feign dedication and commitment; the scammers also present themselves as people with positive attributes. The pattern also showed the grateful nature of the

scammers towards their recipients. The study further reveals that scammers usually hide behind a male identity to carry out their deceptive acts.

The study also demonstrated that cultural, political and social factors influence the choice of language use by speakers or writers. The culture of people could influence them to avoid the use of certain words or expressions which are considered inappropriate in that culture. It was noticed that, some scam email messages contained quotes from the Quran, while others contained quotes from the Bible. It was interesting to note that the scammers' choose to make reference to any these two religions based on the culture they wanted to project in the scam email messages.

5.4 Implications of the Study

This study has implication for the application of transitivity on a text especially on language of deception. Even though previous studies have explored language in different aspects using transitivity as a theory, Ignatieva, and Rodríguez-Vergara (2015), Afrianto, and Seomantri,(2014), this study used the transitivity theory to explore the language of scam email messages. This has helped in the understanding of how scammers express their experiences of their world consciously and unconsciously through the use of language. This study also helps in the understanding of the type of relationship that exists between linguistic form and linguistic cues of deception.

The findings have added a new approach to the study of deception in general This study explored the language of scam email messages using a clause by clause analysis to identity the meanings of patterns and how they reveal the manipulative purpose of scamming. This has added a new way of studying scam emails messages. This approach could be used by scholars who have interest in scam emails to explore different aspects of deception.

5.5 Limitations and Recommendations for Future Research

The study had limitation so some recommendations were given for further research. Based on the research findings, the following recommendations were made.

The study employed Systemic Functional Linguistic (SFL) and was limited to the transitivity framework. Other studies can be conducted on scam emails using other frameworks of SFL such as, the Appraisal framework to provide insights and understanding into oral scam emails in order to reveal how scammers interact with the target recipient.

Furthermore, due to time and space constraints, the data of the study was limited to only forty (40) scam emails. Findings of the study can serve as a basis for a comprehensive study using a larger corpus of scam emails.

5.6 Summary of Chapter

This concluding chapter has summarised the aims, methods and findings of the study. Based on the findings, conclusions have been made in relation to the research questions and implications have been drawn. The chapter concluded with recommendations for future research, which are mainly based on some limitations drawn from the study.

REFERENCES

Adams, S. H. (2002). *Communication under stress: Indicators of veracity and deception in written narratives* (Doctoral dissertation). Virginia Polytechnic and State University.

Afrianto, L. M. I., & Seomantri, Y. S. (2014). Transitivity analysis on Shakespeare's Sonnets. *IOSR Journal of Humanities and Social Science*, 78-85.

Afroz, S., Brennan, M., & Greenstadt, R. (2012, May). Detecting hoaxes, frauds, and deception in writing style online. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 461-475). IEEE.

Altheide, D. L., & Schneider, C. J. (2012). *Qualitative media analysis* (Vol. 38). London: Sage.

Bano, Z., & Shakir, A. (2015). Personal pronouns in" About Us" Section of Online University Prospectus. *Journal of Education and Practice*, *6*(1), 133-139.

Baron, N. S. (2003). Language of the Internet. *The Stanford handbook for language engineers*, 59-127.

Behnam, B., Azabdaftari, B., & Hosseini, A. (2011). A critical analysis of financial fraud spam in English in terms of Persuasive Strategies: Personalization, Presupposition, and Lexical Choices. *Journal of English Studies*, *1*, 15-26.

Blommaert, J., & Omoniyi, T. (2006). Email fraud: Language, technology, and the indexicals of globalisation. *Social Semiotics*, *16*(4), 573-605.

Brown, G., & Yule, G. (1983). *Discourse analysis*. Cambridge university press.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203-242.

Burton, D. (1982). Through glass darkly: Through dark glasses. *Language and literature: An introductory reader in stylistics*, 194-214.

Carlson, J. R., Joey, F., George, J. K., Burgoon, M., Adkins, C. & White. H. (2004). "Deception in computer-mediated communication." *Group Decision and Negotiation,* 13(1), 5-28.

Casañ-Pitarch, R. (2016). Case study on banks' webpages: The use of personal pronouns. *International Journal of Language Studies*, *10*(4).

Chapelle, C. A. (1998). Some notes on systemic-functional linguistics. *http://www.public.iatate.edu/carolc/LONG511/sfl.html.*

Chhabra, S. (2005). *Fighting spam, phishing and email fraud* (Doctoral dissertation, University of California, Riverside).

Chiluwa, I. E. (2006). A critical study of language variation and ideological differences in media discourse in Nigeria. *Ibadan Journal of English Studies*, 87-175.

Choudhury, F. (2014). can language be useful in detecting deception? The linguistic markers of deception in the Jodi Arias interview. *Diffusion-The UCLan Journal of Undergraduate Research*, *7*(2).

Christina, V., Karpagavalli, S., & Suganya, G. (2010). A study on email spam filtering techniques. *International Journal of Computer Applications*, *12*(1), 0975-8887.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cukier, W. L., Cody, S., & Nesselroth, E. J. (2006, January). Genres of spam: Expectations and deceptions. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on* (Vol. 3, pp. 51a-51a). IEEE.

Cukier, W., Ngwenyama, O. K., & Nesselroth-Woyzbun, E. J. (2008). Genres of spam. *Scandinavian Journal of Information Systems*, *20*(1), 1.

December, J. (1997). Notes on defining of computer-mediated communication. *Computer-Mediated Communication Magazine*, *3*(1).

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological bulletin*, *129*(1), 74.

Downing, A., & Locke, P. (2006). *English grammar: A university course*. New York, NY: Routledge.

Driskell, T., Neuberger, L., Driskell, J. E., Burke, C. S., & Salas, E. (2014, September). The Language of Lies: A Content Analytic Approach. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 1328-1331). Sage CA: Los Angeles, CA: SAGE Publications.

Edelson, E. (2003). The 419 scam: information warfare on the spam front and a proposal for local filtering. *Computers & Security*, *22*(5), 392-401.

Edwards, M., Peersman, C., & Rashid, A. (2017, April). Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. In *Proceedings of the 26th International Conference on World Wide Web*

Companion (pp. 1291-1299). International World Wide Web Conferences Steering Committee.

Freiermuth, M. R. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse & Communication*, *5*(2), 123-145.

Fuller, C. M., Biros, D. P., Burgoon, J., & Nunamaker, J. (2013). An examination and validation of linguistic constructs for studying high-stakes deception. *Group Decision and Negotiation*, *22*(1), 117-134.

Galasinski, D. (2000). *The language of deception: A discourse analytical study*. London: Sage Publications.

Hallett, R. E., & Barber, K. (2014). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography*, *43*(3), 306-330.

Halliday, M. (2006). New ways of meaning. *The ecolinguistics reader: Language, ecology and environment*, 193.

Halliday, M. A. (1966). Some notes on 'deep' grammar. *Journal of Linguistics*, *2*(1), 57-67.

Halliday, M. A. K. (1961). Categories of the theory of grammar. *Word*, *17*, 241-292.

Halliday, M. A. K. (1994). Spoken and written modes of meaning. *Media texts, authors and readers: A reader*, *51*, 51-73.

Halliday, M. A. K. (2004). An Introduction to Functional Grammar. Language Arts & Disciplines, 480.

Halliday, M. A. K., & Webster, J. J. (2008). *Complementarities in language*. The Commercial Press.

Halliday, M. A., & Christian, M. I. M. (2004). Matthiessen. *An introduction to functional grammar*.

Halliday, M. A., & Hasan, R. (1976). Cohesion in. *English.* London: Longman

Halliday, M., Matthiessen, C. M., & Matthiessen, C. (2014). *An introduction to functional grammar*. New York NY: Routledge.

Hancock, B., Ockleford, E., & Windridge, K. (2007). An introduction to qualitative research: The NIHR RDS EM/YH.

Hancock, J. T., Curry, L. E., Goorha, S., & Woodworth, M. (2007). On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes*, *45*(1), 1-23.

Hancock, J. T., Gee, K., Ciaccio, K., & Lin, J. M. H. (2008, November). I'm sad you're sad: emotional contagion in CMC. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work* (pp. 295-298). ACM.

Hancock, J. T., Thom-Santelli, J., & Ritchie, T. (2004, April). Deception and design: The impact of communication technology on lying behavior. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 129-134). ACM.

Hasan, R., Matthiessen, C., & Webster, J. J. (2007). *Continuing discourse on language: A functional perspective*. Equinox.

Hasan, R., Matthiessen, C., & Webster, J. J. (2007). *Continuing discourse on language: A functional perspective*. Equinox.

Hauch, V., Blandón-Gitlin, I., Masip, J., & Sporer, S. L. (2015). Are computers effective lie detectors? A meta-analysis of linguistic cues to deception. *Personality and Social Psychology Review*, *19*(4), 307-342.

Herring, S. C., & Stoerger, S. (2014). Gender and (a) nonymity in computer-mediated communication. *The handbook of language, gender, and sexuality*, *2*, 567-586.

Herring, S. C., Barab, S., Kling, R., & Gray, J. (2004). An approach to researching online behavior. *Designing for virtual communities in the service of learning*, *338*.

Hershkop, S., & Stolfo, S. J. (2005, August). Combining email models for false positive reduction. In *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining* (pp. 98-107). ACM.

Hershkop, S., & Stolfo, S. J. (2006). *Behavior-based email analysis with application to spam detection*. Columbia University.

Hildebrandt, L. (2015). Media and Self Representative Perceptions: Deception in Online Dating.

Hinde, S. (2005). Identity theft: Theft, loss and giveaways. *Computer Fraud & Security*, *2005*(5), 18-20.

Hiß, F. (2015). Fraud and Fairy Tales: Storytelling and Linguistic Indexicals in Scam E-mails. *International Journal of Literary Linguistics*, *4*(1).

Holt, T. J., & Graves, D. (2007). A qualitative analysis of advance fee fraud email schemes. *The International Journal of Cyber Criminology*, *1*, 137-154.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research*, *15*(9), 1277-1288.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research*, *15*(9), 1277-1288.

Humpherys, S. L., Moffitt, K. C., Burns, M. B., Burgoon, J. K., & Felix, W. F. (2011). Identification of fraudulent financial statements using linguistic credibility analysis. *Decision Support Systems*, *50*(3), 585-594

Hunston, S. (2010). How can a corpus be used to explore patterns. *The Routledge handbook of corpus linguistics*, 152-166.

Ignatieva, N., & Rodríguez-Vergara, D. (2015). Verbal processes in academic language in Spanish: exploring discourse genres within the systemic functional framework. *Functional Linguistics*, *2*(1), 2.

Isacenkova, J., Thonnard, O., Costin, A., Francillon, A., & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security*, *2014*(1), 4.

Jiménez Bernal, M., & Belli, S. (2013). Virtual ethnography and spam: Fraud and Fear in deceptive narratives on the Internet.

Kerkeb, A. (2013). A genre analysis of business English e-mails the case of a multinational's Algerian employees. *Dr. Manoj Kamat (India)*, *79*.

Martin, J. R. (2016). Meaning matters: A short history of systemic functional linguistics. *Word*, *62*(1), 35-58.

Masip, J., Garrido, E., & Herrero, C. (2004). Defining deception. *Anales de Psicología/Annals of Psychology*, *20*(1), 147-172.

Matthiessen, C. M. (2007). The 'architecture' of language according to systemic functional theory: Developments since the 1970s.

Matthiessen, C. M. I. M. (2007). Lexicogrammar in systemic functional linguistics: descriptive and theoretical developments in the 'IFG' tradition since the 1970s. *Continuing discourse on language: a functional perspective*, *2*, 765-858.

McCarthy, M. (1991). *Discourse analysis for language teachers*. Cambridge University Press.

Mehrpour, S., & Mehrzad, M. (2013). A comparative genre analysis of English business e-mails written by Iranians and native English speakers. *Theory and Practice in Language Studies*, *3*(12), 2250.

Mihalcea, R., Pérez-Rosas, V., & Burzo, M. (2013, December). Automatic detection of deceit in verbal communication. In *Proceedings of the 15th ACM on International conference on multimodal interaction* (pp. 131-134). ACM.

Mwinlaaru, I. N., & Xuan, W. W. (2016). A survey of studies in systemic functional language description and typology. *Functional Linguistics*, *3*(1), 8.

Naksawat, C., Akkakoson, S., & Loi, C. K. (2016). Persuasion strategies: use of negative forces in scam e-mails. *GEMA Online® Journal of Language Studies*, *16*(1).

Newman, M. L., Pennebaker, J. W., Berry, D. S., & Richards, J. M. (2003). Lying words: Predicting deception from linguistic styles. *Personality and social psychology bulletin*, *29*(5), 665-675.

Ottenheimer, H., & Ottenheimer, D. (2006). Urgent/Confidential–An Appeal for Your Serious and Religious Assistance: The Linguistic Anthropology of "African" Scam Letters. *The anthropology of language. An introduction to linguistic anthropology. Belmont: Wadsworth*, 213-227.

Patton, M. Q., & Cochran, M. (2002). A guide to using qualitative research methodology. *Medecins Sans Frontiers. Retrieved February*, *14*, 2014.

Pennebaker, J. W., Boyd, R. L., Jordan, K., & Blackburn, K. (2015). *The development and psychometric properties of LIWC2015*.

Pérez-Rosas, V., Abouelenien, M., Mihalcea, R., Xiao, Y., Linton, C. J., & Burzo, M. (2015, September). Verbal and Nonverbal Clues for Real-life Deception Detection. In *EMNLP* (pp. 2336-2346).

Rabon, D. (2003). *Investigative discourse analysis*. Carolina Academic Press.

Rich, T. You can trust me: a multimethod analysis of the Nigerian email scam. *Security Journal*, 1-18.

Rodríguez, G. A. (2008). *Second language sentence processing: Is it fundamentally different?* (Doctoral dissertation, University of Pittsburgh).

Romiszowski, A., & Mason, R. (1996). Computer-mediated communication. *Handbook of research for educational communications and technology*, *2*, 397-431.

Salvetti, F., Lowe, J. B., & Martin, J. H. (2016). A Tangled Web: The Faint Signals of Deception in Text-Boulder Lies and Truth Corpus (BLT-C). In *LREC*.

Shafqat, W., Lee, S., Malik, S., & Kim, H. C. (2016, April). The language of deceivers: Linguistic features of crowdfunding scams. In *Proceedings of the 25th International Conference Companion on World Wide Web* (pp. 99-100). International World Wide Web Conferences Steering Committee.

Simpson, P. (2004). *Stylistics: A resource book for students*. Psychology Press.

Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). *Nigerian advance fee fraud*. Canberra: Australian Institute of Criminology.

Stern, R. M., Ray, W. J., & Quigley, K. S. (2001). *Psychophysiological recording*. Oxford University Press, USA.

Swales, J. (1990). *Genre analysis: English in academic and research settings*. Cambridge University Press.

Tabron, J. L. (2016). *Creating urgency in tech support scam telephone conversations* (Doctoral dissertation, Hofstra University).

Tan, H. K., & David, Y. (2017). Preying on lonely hearts: A systematic deconstruction of an internet romance scammer's online lover persona. *Journal of Modern Languages*, *23*(1), 28-40.

Thompson, G. (2013). *Introducing functional grammar*. London: Routledge.

Toma, C. L., & Hancock, J. T. (2012). What lies beneath: The linguistic traces of deception in online dating profiles. *Journal of Communication*, *62*(1), 78-97.

Trappes-Lomax, H. (2004). Discourse analysis. *The handbook of applied linguistics*, 133-164.

Tsikerdekis, M., & Zeadally, S. (2014). Online deception in social media. *Communications of the ACM*, *57*(9), 72-80.

Vrij, A., Edward, K., Roberts, K. P., & Bull, R. (2000). Detecting deceit via analysis of verbal and nonverbal behavior. *Journal of Nonverbal behavior*, *24*(4), 239-263.

Yoo, K. H., & Gretzel, U. (2009). Comparison of deceptive and truthful travel reviews. *Information and communication technologies in tourism 2009*, 37-47.

comparison of classification methods for predicting deception in computer-mediated communication. *Journal of Management Information Systems*, *20*(4), 139-166.

Zhou, L., Twitchell, D. P., Qin, T., Burgoon, J. K., & Nunamaker, J. F. (2003, January). An exploratory study into deception detection in text-based computer-mediated communication. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on* (pp. 10-pp). IEEE.

APPENDICES