Chapter 22
"Attention Beneficiary...!": Assessing Types and Features of Scam Emails

Innocent E. Chiluwa
Covenant University, Nigeria

Ebikaboere Ovia
Covenant University, Nigeria

Emmanuel Uba
Covenant University, Nigeria

ABSTRACT

This chapter identifies the various types and features of scam emails as a genre of computer-mediated communication. The types identified include money transfer, investment scam, inheritance claim, next-of-kin claim, charity donation scam, foreign aid scam, foreign lottery scam and email account lottery scam. The study also describes the linguistic and discourse features of these types of scam emails and argues that the more knowledge of online financial crimes that is created and disseminated, the more people are informed and empowered to protect themselves against them. This study hopes to contribute significantly to literature on phishing attacks and online financial crimes.

INTRODUCTION

Scam is synonymous with fraud, dishonesty or treachery. Like other types of phishing, "scam emails" refers to unsolicited emails that aim to defraud the receiver by tricking them into disclosing their bank details or other private security information. Phishing emails may appear in graphical form or in both written and pictorial formats. From ancient times, it appears that some people are endowed with sugar-coated tongues or are gifted with the exceptional ability to lie or tell stories that can deceive others. Before the advent the Internet, business scams or "confidence games" came in similar forms, suggesting business ideas or offering partnership in an already existing one. These "business deals" might involve financial commitments, where postal costs were incurred, and other risks such as letters being lost in transit, being

DOI: 10.4018/978-1-5225-8535-0.ch022

delayed in delivery or being sent to a wrong person were experienced. However, as awareness of business scams grew among business people, some scam mails were intercepted in the process of mailing and discarded; in some cases, where writers of scam mails were arrested, they were tried and imprisoned.[1]

Information technology and the Internet now make online fraud or email scams much easier and faster since its delivery to the target is almost instantaneous and occurs without an intermediary. It also retains confidentiality as it is not made public, except by the recipient.

The Internet further allows for sourcing of any kind of information and accessing other contacts through an initial contact, among other benefits to the scammer. Thus, criminal-minded persons have likely targets for their emails available on a daily basis. As an updated version of the pre-Internet confidence game, scam email removes the risk of seeing face to face, making crime easier to commit at this stage, insofar as facial and body gestures are eliminated or postponed.

The present study focuses on scam emails also known as "Nigerian 419 emails" or "advance fee fraud" (Chiluwa 2009; 2010). Recipients of such unsolicited emails are either offered a money donation or asked to partner with other persons to transfer a specified huge amount of money for a fee; sometimes recipients are asked to utilize some money that would be made available to them for some charity work. In the context of this study, scam emails are differentiated from the general spam emails in terms of their criminal intent and has actually resulted in scams, where unsuspecting victims have been defrauded of their money (Chiluwa 2015). In 2016, about $59 million were lost to investment scams in Australia alone, and it is estimated that losses will exceed US$1 trillion globally (See Chiluwa 2019; Vishwanath et al, 2011).

BACKGROUND

Studies in linguistics, law, cybercrime and cybersecurity have recognized the menace of phishing and email scams, many of which are said to originate in Nigeria (Heyd, 2008). Zook (2007, p.65) particularly argued that advance fee fraud "has strong historic ties to Nigeria" with a global network that operates in other countries. Email scams by Nigerians have been said to be justified as a way of providing reparations for crimes against Africans, who were cheated through slave trade and colonialism. This argument has assisted scammers to rationalize their crimes, convincing themselves that scamming is justifiable given these special circumstances. The idea of Nigerians being the kingpins of scam reached such an embarrassing height that the Nigerian Government formulated a legal injunction about scam being punishable by law. "419", which has come to be known as a synonym for scam, is a section of the Nigerian criminal code, dealing with advance fee fraud (Chiluwa, 2010).

The first studies of email scams adopted linguistic approaches to investigate the English competence of the writers of scam emails for a clue to the origin of the scammers (see Blommaert, 2005). Also, Blommaert & Omoniyi (2006) argued that while the authors of scam emails demonstrated technical skills in the use of information technology, they lacked the corresponding linguistic competence to produce the appropriate messages to reflect the credible identities and relationships in the proposed transactions. More recently, however, Taiwo (2012) argued that scammers had "improved" in terms of how the messages were constructed.

According to that study, the scam email writers relied on experiential knowledge of the recipient's vulnerability and constructed their messages to appeal to them. Hence, certain scam emails used fewer pressure tactics, and writers tend to construct for themselves an identity of a "non-confident, naïve,