Journal of Emerging Technologies (JET)
Volume 4, Issue 2 (2024)
ISSN: 2710-0189 (Print) | 2710-0197 (Online)
Website: https://journals.jozacpublishers.com/jet/
https://doi.org/10.57040/z07jkm33

Uncovering cybercrime tactics: Studying emerging linguistic features and forms of Swahili fraudulent SMS in Tanzania

Lazaro Charles[1*]

[1]*Department of Linguistics and Literary Studies, The Open University of Tanzania, Tanzania,* lazarocharles55@gmail.com

*Corresponding author: lazarocharles55@gmail.com

Abstract: The majority of Tanzanians have fallen victim to cybercrime committed by imposters via SMS, the popular short messaging service. The victims have been tricked into sending money or engaging in fraudulent activities by those SMSs. The current research set out to study the fraudulent SMSs sent among Tanzanians. The study was guided by two objectives: firstly, to identify the forms of fraudulent SMSs, and secondly, to uncover their distinguishing features. A total of 97 fraudulent SMSs were collected from diverse recipients, including the author of this paper, and subjected to qualitative analysis. The linguistic stylistic approach guided the data analysis of the study. The study reveals several forms of fraudulent SMSs, including money transfers, superstition, easy money making, rental and landlord, fake lotteries, extortion, and false employment offers. Furthermore, the study identifies some features contained in those SMS, such as the absence of formal salutations, the sender and recipient's anonymity, typographical errors, distinctive writing styles, and the lack of politeness markers. Money-making and social problem-solving promises, extorting, hiding the purpose of money transfers, and impersonation are a few more. The study recommends that to reduce the chances of becoming a victim of fraud orchestrated by cybercriminals, recipients of these SMSs should exercise caution and critical judgment when receiving such SMSs.

Keywords: Cybercrime, Fraud and fraudsters, Linguistic Stylistics, Scam, Swahili fraudulent SMS

1. Introduction

In the contemporary era, we are witnessing a rapid expansion of information technology, greatly simplifying various aspects of life. This expansion has simplified online business transactions, and financial operations, and even facilitated distant participation in political processes such as voting, as noted by Akbar (2014). However, scholars like Chete et al. (2012) and Mat-Dangi and Tajuddin (2013) claim that the development of information technology has sparked the emergence of novel forms of criminal activity, including cybercrimes such as identity theft, online fraud, and hacking, notwithstanding its expediencies in everyday life. Amongst these technological developments, social media stands out as a platform often utilised for evil purposes, including cyberbullying and harassment (Çakar-Mengü & Mengü, 2023; Maurya, 2023; Zubair, Zubair & Ahmed, 2023). Social media has become a fruitful ground for criminals, particularly fraudsters, who use it to execute fraudulent schemes and deceive imprudent people. Driven by financial hardships, some individuals resort to leveraging technological innovations to engage in illegal activities as a means of financial sustenance (Lyons, 2019). Fraud, in its various forms, can be committed by anyone. The current study, specifically, examines one such instance of fraud affecting telecommunication services—the use of fraudulent SMS—a topic deserving investigation within the developing information technology landscape.

A fraudulent message or short messaging service (SMS) is a deceitful message sent through a mobile device, typically with the deceptive goal to the recipient (Brown, 2005). The senders of such messages often pose as reputable entities such as governmental bodies, banks, or established businesses, beseeching sensitive financial details, and personal information, or instigating actions such as transferring money to false bank accounts, clicking on malevolent links, or sending money to unidentified parties. Short text messages have certainly transformed how fraudsters work. The speed and anonymity of these messages, coupled with their capacity to reach a widespread audience quickly, enable fraudsters to operate on a large scale within a very short time (Mat-Dangi & Tajuddin, 2013). Recipients are entrapped by fraudulent SMS through various tactics, including exploiting curiosity, fear, or trust. Fraudulent SMSs are circulated in huge quantities to numerous recipients, taking advantage of variations in understanding the traits of these SMSs. As a result, many people have fallen victim to fraudsters, incurring diverse costs, mainly financial, with some even becoming involved in secret associations related to fraud (Liu et al., 2021). Plentiful cases of fraudulent SMS have been reported and documented in the media. For instance, Mat-Dangi and Tajduna's (2013) study reports a case in Indonesia where Subex Telecol1 Fraud Alerts documented a case involving a senior executive of a telecom operator suspected of involvement in a premium rate SMS scam, resulting in criminals illegally obtaining $1.3 million monthly in 2012. The same study reports another case in France where two individuals were arrested for developing mobile malware and scams that conned users, making them accumulate nearly 100,000 euros in total. These cases illustrate the magnitude of fraudulent activities, which are capable of imposing substantial losses on service providers and their customers alike.

Narratives about SMS-related frauds are widespread in Tanzania, where various people have encountered deceptive SMSs aimed at perpetrating fraudulent activities (Tanzania Communications Regulatory Authority, 2023). Given the extensive usage of SMS in the country, the likelihood of falling victim to fraud via SMS is notably high. These fraudulent schemes not only impose financial losses upon recipients but also subject them to psychological distress (Mat-Dangi & Tajduna, 2013). Motivated by the persistence of these fraudulent SMSs and their detrimental impact (Duha, 2021; Tanzania Communications Regulatory Authority, 2023), the author embarked on a study aimed at raising awareness about the writing styles used by these fraudsters as these SMSs are delivered to various people on a daily basis and individuals continue to be deceived. The dissemination of such information is crucial as it empowers Tanzanians to identify these deceptive SMSs and refrain from making potentially costly decisions. The current study examines the forms and linguistic features employed by Tanzanian fraudsters in crafting their SMSs. By familiarising themselves with these forms and features, recipients have a better chance of recognising these SMSs, which may reduce the incidence of crimes committed through such SMSs.

2. Literature review

Studies on cyber fraud have been conducted in various parts of the world, focusing mainly on email fraud, although other studies have also investigated fraud committed through SMSs. One such study was conducted by Onanuga (2017) who examined the distinguishing linguistic features of Nigerian spam SMSs. Using linguistic stylistic analysis, the study categorised Nigerian spam SMSs into several categories such as sports updates, bank notifications, promotional offers, network/service provider messages, religious SMSs, and health. The study revealed the features contained in these SMSs such as the use of internet text notations, code-mixing, graphological deviations, textese, and disregarding punctuation rules. The study further reveals that such messages were found to be persuasive, employing techniques like polite salutations, inducement, "call-to-action" verbs, and emotive language. Another study was conducted by Nlebedum (2017) whose research examined scam emails that were sent to the customers of Diamond Bank and Guaranty Trust Bank in Nigeria, alongside genuine bank emails from both banks. The study aimed to determine the possibility of discrepancy in authorship features between scam emails and genuine bank emails. The study found unique features in scam emails that were not found in genuine mails. Pervaiz et al. (2019) studied SMS fraud in Pakistan by identifying and categorising fraudulent messages as well as their impact on those who receive them. The study found that lottery fraudulent SMSs dominated in Pakistan. The study further established that these schemes greatly impacted the vulnerable rural and low-income populations.

In 2019, Parsons et al. investigated the factors influencing the success of email phishing attacks and the susceptibility of individuals to such emails. The study used a social influence framework and the Susceptibility to Persuasion Strategies scale within a dual-process model of persuasion framework. The study established that phishing emails that employed scarcity and social proof principles were least successful while

those that employed reciprocity and consistency principles were most successful. Similar principles were also considered least and most persuasive based on the Susceptibility to Persuasion Strategies scale. For the majority of principles, participants who were vulnerable to a particular principle were remarkably more liable to emails containing that principle. Moreover, the study demonstrated that susceptibility to the social proof principle; the percentage of time spent using a computer; both dispositional and situational impulsivity; and age, were the main factors for people's capability to recognise phishing email. In the same year, Lin et al. studied the effects of internet user age and email content as weapons of influence on spear-phishing susceptibility. The study involved 58 older and 100 young users (without their knowledge) for 21 days. The study showed that 43% of users fell for the simulated phishing emails, with older women being the most susceptible. Older users showed stable susceptibility while young users showed declined susceptibility. The relative effectiveness of the attacks differed by weapons of influence and life domains with age-group variability. The efficacy of the attacks varied by weapons of life domains and influence alongside age group variability. The study further revealed that older users demonstrated lower susceptibility awareness compared to young ones.

In 2007, Holt and Graves used a sample of 412 fraudulent e-mail messages to examine the mechanisms used by scammers. Their study indicated the presence of multiple writing techniques that were used to produce responses and information from victims. Their study also indicated that half of all e-mails requested recipients to forward their personal particulars to the sender, which enabled identity theft. Alake's (2017) study investigated the pragmatic functions of a style of the selected Nigeria Electronic Advanced Fee Fraud texts using Pragma-Stylistics. The study purposively selected and randomly stratified a sample of 50 from a population of 1,200 texts collected from www.fraudgallery.com. Among others, the study revealed that cybercrime is a sub-genre of advertisement. On the other hand, Ajayi (2022) studied the discursive-manipulative strategies found in scam emails and SMSs in Nigeria. The study involved samples from a corpus of over 200 emails and 50 SMS collected between 2018 and 2022. The study was analysed based on Brown and Levinson's face, Mey's pragmatic act, and McCronack's information manipulation theories. The study established that discursive manipulative strategies such as self-denigration, formulaic, positive and negative false alarms, and evocation of theistic and religious context characterised the Nigerian scam emails and SMS. The findings further showed that face-saving and face-threatening acts were strategically entrenched in these manipulative strategies to enable the flouting of the maxims of quantity and quality.

Despite all the efforts in research, cybercrimes through mail and SMSs are still widespread across communities, Tanzania included. Given the increasing incidence of fraudulent SMS within Tanzanian society, a thorough investigation of the forms and distinguishing features of these SMSs is crucial. The findings of this study provide Tanzanians with enhanced insights into the forms and fundamental features of fraudulent SMS, which will enable them to identify them (fraudulent SMSs) and take necessary caution to avoid falling prey to these scammers' practices.

3. Theoretical framework

The current study is based on the Linguistic Stylistics theory (also known as Linguistic Criticism, Fowler, 1986; or Stylistic Analysis, Leech, 1969). This theory focuses on studying stylistic devices contained in certain texts (Ayeomoni, 2003). Stylistic analysis in linguistics involves the orderly evaluation of discourse and language patterns in a certain speech or text to identify its distinctive stylistic features such as figurative language, tone, sentence structure, diction, and others. This approach aims at understanding how language is used to create meaning and prompt certain responses from the audience. The approach contributes to the description and interpretation of texts as generative stylisticians such as Chapman and Clark (2014) and Thorne (1983) emphasise. This approach is relevant to the current study as it leads to understanding how language is used to communicate meaning and identify communication goals within fraudulent SMS. Thus, the approach helps in examining the forms and linguistic features contained in these SMSs and their contribution to the overall communicative goal.

4. Methodology

The current study used a descriptive research design. The study used a qualitative approach – a research approach which involves non-numerical data to produce insights about a studied phenomenon (Ugwu & Eze, 2023). It is a research approach that provides findings not derived from statistical procedures or other means of quantification (Strauss & Corbin, 1990). The qualitative data were collected from various people who

received fraudulent SMS, including the author of this paper. The data collection process involved asking people from various WhatsApp groups to share with the author any fraudulent SMS they received. Using WhatsApp groups enabled the author's request to reach many people. The data collection process took four weeks (from the second week of October 2023 to the second week of November 2023). During this time, a total of 97 fraudulent SMSs were collected. Collecting such SMS was not easy as most recipients tend to delete them immediately after receiving them. Despite this challenge, the nature of the research made this sample sufficient, as the content and linguistic features of the collected SMSs showed great similarity. Also, the sample size was deemed reasonable as it made the analysis manageable while ensuring sufficient data for the research objectives. The collected data were qualitatively analysed to identify the forms and unique linguistic features contained in fraudulent SMS sent by fraudsters among Tanzanians. The data analysis involved a careful examination and interpretation of the collected SMSs which enabled the identification of various forms and linguistic features of the collected fraudulent messages. Afterward, the results were presented qualitatively, accompanied by descriptive statistics to provide additional insight into the findings.

5. Results and discussion

The findings are presented and discussed in the following sections. The presentation of the forms of fraudulent SMSs that have been identified opens this section, followed by a presentation and discussion of the observed features of the fraudulent SMSs. Examples in these data are presented as they are, even if they contain certain typographical errors, to exactly depict the way these SMSs are written by the imposters.

5.1. Forms of fraudulent SMSs

In this study, different forms of fraudulent SMSs are identified, which are presented in *Figure 1*.

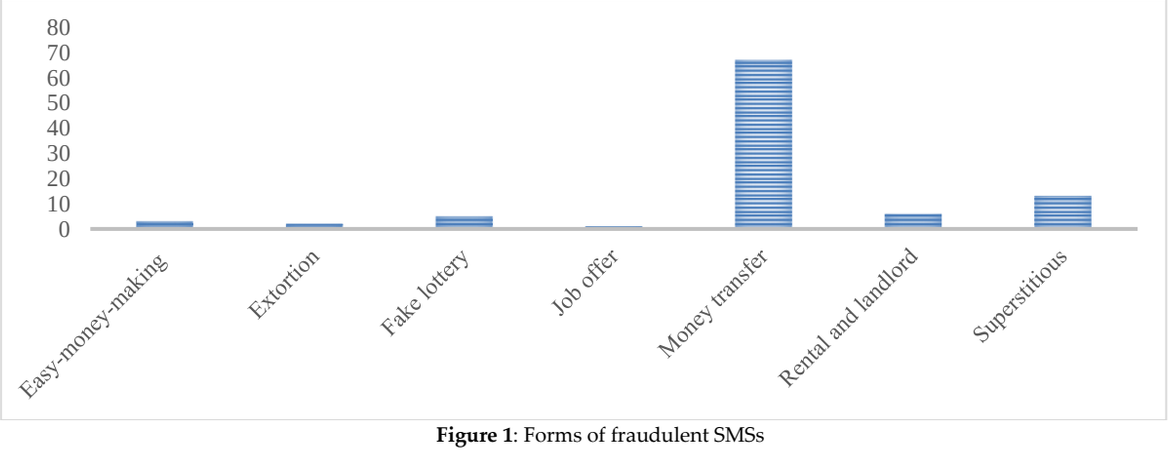

Figure 1: Forms of fraudulent SMSs

The sections that follow describe these forms.

Money transfer SMSs

These are SMSs that were sent to different individuals, luring them to send money to the senders of these SMSs. This category constitutes 69% of all SMSs received, as depicted in *Figure 1*. Considering the number of these SMSs, this percentage is notably high. It highlights the effectiveness of this form of SMS in deceiving recipients. Among these SMSs, 68.7% prompted recipients to send money via Airtel numbers. This suggests the presence of security weaknesses in the Airtel mobile network that allow cybercriminals to commit their crimes without being noticed. Presented below is an example of such an SMS:

Niwekee iyo hela kwenye hii Airtel 0788544489 NEEMA MBUKWA
Credit for me the money on the Airtel 0788544489 NEEMA MBUKWA

Superstious SMSs

These deceptive SMSs are aimed at luring people into contacting self-proclaimed traditional healers who supposedly offer solutions to various personal issues. These SMSs constitute a significant portion, comprising 13.4% of all SMSs collected, as illustrated in *Figure 1*. This percentage underlines the prevalence of such category of fraudulent SMSs. These SMSs are generally distributed to a wide range of recipients who may be

experiencing challenges that the fraudsters falsely claim to address. It is likely that these scammers have already victimised numerous people, prompting them to send as many of these SMSs as possible. The promises made by these traditional healers include facilitating marriage, reconciling estranged spouses, removing misfortune, and promising wealth acquisition. People who are ambitious of such assurances may fall prey to such deception and fraud. Presented below is an example of such SMSs:

kumiliki Mari bira kafara.kupata kazi.masomo.kumrudisha mke au mme.nyota,kesi.uzazi.biashara.pete.nk.kama unashida piga (0689037067)
To own property without sacrifice.getting a job. (passing in) studies.bringing back a wife or husband.horoscope, cases.birth.business.rings.etc. if you have problems call (0689037067)

Rental and landlord SMSs

These are SMSs designed to persuade recipients into transferring money to individuals posing as landlords, who are in reality fraudsters. These SMSs are delivered to various recipients, with the senders aware that some of the receivers may be tenants under certain landlords. Typically, such SMSs inform recipients that their rent payment is overdue, relying on the likelihood that some tenants may indeed be in such a situation. Despite the relatively low occurrence of such SMSs, as depicted in *Figure 1*, there is a possibility that recipients have fallen victim to these fraudulent schemes. To dwindle such scams, it is imperative to comprehend the nature and characteristics of these SMSs. An example of such an SMS is provided below:

Habari za leo mimi mzee wako mwenye nyumba vip mbona kimya na tarehe zinazid Kwenda.
Greetings, I am your landlord, why so quiet and the dates keep passing by.

This form of fraudulent activity is not confined to Tanzania only but is rather widespread across the globe. According to the UK National Fraud Authority's assessment, rental scams was estimated to ensnare approximately 315,000 people annually, with an average financial loss of £2,394 per victim, leading to a cumulative annual loss amounting to £755 million (National Fraud Authority, 2014).

Fake lottery SMSs

SMSs falling into this category deceitfully inform recipients that they have been awarded a certain amount of money through a lottery, even if they have not participated in any lottery. In an attempt to lure recipients, the fraudsters advertise substantial winnings supposedly available through these fictitious lotteries. Subsequently, the senders (fraudsters) direct recipients to call a separate number provided in the SMS to receive instructions on claiming the allegedly "won" money. Faluyi, Fele, and Ayemi (2020) and Onanuga (2017) encountered a similar type of SMS while examining spam SMS in Nigeria and the latter referred to them as bonanza or jackpot SMSs. Although the proportion of these messages is relatively small, as depicted in *Figure 1* (5.2%), this does not negate the possibility of individuals receiving them to be victimised by such frauds. Recipients need to be cautious to prevent falling for such a fraud. Presented below is an example of such SMSs:

[HALO WINI] Hongera!! Umezawadiwa Tsh 7,000,000.00 MILIONI SABA kutoka HALOTEL kampuni no.1155 Piga simu TCRA no.069669497 Ujaziwe form yako Ahsante
[HELLO WINI] "Congratulations!! You have been awarded Tsh 7,000,000.00 SEVEN MILLION from HALOTEL company no.1155 Call TCRA no.069669497 Fill in your form Thank you

Easy money-making SMSs

Only 3.1% of the total fraudulent SMSs collected fall into this category. These SMSs tempt recipients to join certain associations, such as the Freemasons, promising quick wealth and prosperity. However, these SMSs are merely mechanisms to deceive those who receive them. The senders of these SMSs instruct those interested in joining these associations to call the provided number for further details and instructions. Many individuals have fallen victim to these fraudsters in their pursuit of a lavish lifestyle, driven by life's challenges and the desire for rapid wealth acquisition. Regrettably, their aspirations often result in deception. Below is an example of such SMSs:

JIUNGE FRIMASON UWEZE KUMILIKI PESA MAJUMBA NA MAGARI YA KIFAHARI KUKUZA BIASHARA,VIPAJI PIGA NAMBA 0733584411 KAMA UKO TAYARI KUJIUNGA
JOIN FREEMASON YOU CAN OWN MONEY HOUSES AND LUXURIOUS CARS TO DEVELOP BUSINESS, TALENT CALL 0733584411 IF YOU ARE READY TO JOIN

Extortion SMSs

Extortion fraud constitutes a criminal offense wherein individuals or organisations employ intimidation, coercion, or threats to extract assets, cash, services, or other advantages from a victim (Rose-Ackerman, 2010). In the context of the present study, certain SMSs were observed wherein prosperous individuals were intimidated into transferring money to fraudsters posing as witch doctors or magicians who supposedly facilitated their wealth acquisition through superstition. These threats are typically premised on the notion that the fraudsters aided the victims in achieving prosperity but allege that certain agreed-upon conditions were not met. Consequently, they resort to threats of harm or supernatural impoverishment. As depicted in *Figure 1*, these SMSs constitute only 2.1% of all fraudulent SMSs collected. This implies a relatively low success rate for fraudsters utilising these SMSs, possibly due to the heightened awareness and discernment exhibited by many economically successful individuals (Brown & Reynolds, 1975; Wachtel, 1976), making them less susceptible to scams. Nevertheless, it is imperative to remain cautious against such SMSs and undertake appropriate precautionary measures. Below is an example of one of these SMSs:

super feo nasikitika sana nimekupa ndangu na umefuata masheriti na umepata utajili mkubwa na unaniheshimu babu yako ukumbuke wewe na wenzako mwendamseke manyanya na huyu chijana wa Mwanza nimemusaidia ila kwa heshima yako nimemusaidia amefanikiwa hataki kuja kushukuru ananitumia pesa tu mwambie asione magari yake na nyumba alizojenga kafika anaweza baki bila kitu na wewe badilisha dawa kwenye mabasi yote patakuku mweusi uchinje damu mwagia katika mto wamaj
super feo, I am very sorry that I gave you my charm and you have followed the rules and you have become prosperous and you respect me, your witch doctor, remember that you and your colleagues mwendamseke manyanya and this young man from Mwanza, I have helped him just to respect you, I have helped him. He is now successful but he does not want to come to thank me; he is just sending me money; tell him I have power to dispossess him with everything he owns. And you change the charm for your buses; slaughter the black chicken and pour its blood in the river

False job offer SMSs

As Slaney (2024) elaborates, this category of fraudulent SMS involves fraudsters acting as companies pretending to offer job opportunities to job seekers only to lure the prospective employers searching employees. Within the dataset, only one instance of such an SMS was identified, comprising 1% of all fraudulent SMSs collected. In this SMS, the fraudsters advertise "job vacancy" and promise prospective applicants immediate salary payments upon securing the job. Below is an example of such an SMS.

Ndugu naomba unitafutie kijana awetandiboi wangu kwenye lori kutokea mikoani akipatikana nijulishe analipwa na ofisi zetu kampuni azam awe muaminifu
Please find for me someone to be my turnboy in a truck operating from upcountry. If found, let me know he is going to be paid by our offices Azam company he must be an honest person

This SMS is evidently fraudulent. The discrepancy between the purported company's brand, the platform used to advertise the vacancy, and the typographical errors within the SMS strongly indicate the deceptive nature of this SMS, rather than any genuine attempt to address the employment crisis. It is somewhat perplexing that the senders of such SMS—who are scammers—are seeking individuals of high integrity. However, given the quantity of SMSs gathered and the diverse forms of fraudulent SMSs outlined in preceding sections, this particular fraud technique appears to yield minimal success. Nevertheless, this does not diminish the importance of taking caution when encountering such SMSs, as individuals may still fall prey to these scammers, particularly in the midst of the prevalent issue of unemployment.

The subsequent sections delineate and analyse the features of these SMSs. By identifying these attributes, recipients of such messages can become informed and equipped to minimise the risk of falling prey to these fraudulent schemes.

5.2. Features of fraudulent SMSs

Fraudulent SMSs may exhibit varying characteristics, depending on the specific form of the SMS. Following the exhaustive observation and analysis of the collected SMSs, the prominent features outlined below were evident.

Absence of formal salutations

Formal salutations serve as a fundamental aspect of effective communication (Akindele, 2007; Dzameshie, 2002). Typically, genuine SMSs exhibit a degree of courtesy by commencing with salutations. Interestingly, none of the fraudulent SMSs collected commenced with such salutations. The absence of formal greetings is a red flag indicating the dubious nature of the message's origin. Consequently, it is advisable to exercise caution and thoroughly scrutinise any received SMS before making any decisions, ensuring satisfaction regarding its authenticity. Presented below is an example of one of these fraudulent SMSs.

nitumie kwenye namba hii ya airtel 0788828268 jina litakuja MARIAGORETHA MWANISAWA
send me (the money) on this airtel number 0788828268 the name will come MARIAGORETHA MWANISAWA

As evidenced in the SMS just provided, the sender neglected to extend formal greetings to the recipient(s), a trend consistent across all fraudulent SMSs examined. While the absence of salutations alone may not definitively categorise the SMS as fraudulent, it raises suspicions regarding its authenticity. Recipients of such SMSs should exercise necessary precautions to prevent potential fraudulence.

Anonymity of the sender

Although most democratic nations regard anonymity as a cornerstone of free speech (Scott, 2004), employing this tactic in communication is also associated with other concerns, including spam (Crews, 2007). Upon analysing the collected SMSs, it was observed that not a single sender identified themselves by names. The anonymity of the sender can potentially confuse recipients, rendering them susceptible to victimisation by fraudsters. Hence, individuals receiving SMSs with this characteristic should carefully assess the content before making any potentially costly decisions. Consider the following example:

ILE KODI YA NYUMBA NITUMIE KWENYE NAMBA HII YA VODA 072479632 JINA LITAKUJA KASHESHE MANGULA..USITUMIE ILE YA AIRTEL MAANA SIMU IMETUMBUKIA CHOONI! AHSANTE
SEND ME THE HOUSE RENT TO THIS VODA NUMBER 072479632 THE NAME WILL COME KASHESHE MANGULA..DO NOT USE THE AIRTEL ONE BECAUSE THE PHONE DROPPED IN THE TOILET! THANK YOU

In this excerpt, the fraudster assumes the identity of a landlord but refrains from disclosing their name. This deceptive tactic can mislead the recipient, particularly if they happen to be a tenant, potentially resulting in the transfer of money to the provided number. Therefore, exercising utmost caution when responding to such SMSs is imperative to avoid falling victim to fraudulent schemes.

Anonymity of the recipient

A notable proportion of the fraudulent SMSs examined not only obscured the identity of the senders but also omitted identifying the recipients. This lack of recipient identification leaves the receiver uncertain whether they are the intended target of the SMS. Consequently, this ambiguity makes recipients more susceptible to the tactics of fraudsters. Therefore, to mitigate the risk of falling victim to a scam, individuals should take caution when encountering an SMS with this characteristic. Examine the following example:

iyo ela nitumie kwa hii Airtel 0697193027 jina DEVOTHA MLINGO
send me that money to this Airtel 0697193027 name DEVOTHA MLINGO

As it is seen from the provided SMS, the sender's identity is concealed. Furthermore, the sender attempts to provide a name (that would appear in case money is transferred) that may not be authentic. Similarly, the identity of the receiver remains undisclosed, complicating the determination of the intended recipient of the

SMS. The anonymity of both sender and receiver in such SMSs serves as a warning sign, necessitating precautionary measures to prevent the possibility of making costly decisions.

Typographical errors

The majority of the SMSs examined exhibited numerous typographical errors. While the presence of such errors alone does not conclusively denote fraudulent activity, their abundance, particularly if widespread, serves as a cautionary indication that necessitates careful consideration. The following are the prevalent typographical errors observed:

Beginning sentences with lowercase letters: The predominant characteristic observed in the analysed fraudulent SMSs was the commencement of sentences with lowercase letters, contravening established norms of writing etiquette. Consequently, prior to adhering to instructions provided in a specific SMS, particularly those enticing money transfers, it is imperative to meticulously review the content, especially those arousing doubt. While this feature alone may not suffice to decisively classify a particular SMS as fraudulent, recipients of such SMSs should exercise utmost caution to evade potential victimisation by fraudsters. Consider the following SMS for reference:

iyo ela nitumie kwa hii Airtel 0696724867 jina linakuja SAFARI MWANGORE
send me that money to Airtel 0696724867 the name will come SAFARI MWANGORE

Scriptio continua: Termed "continuous script" in Latin, certain SMSs examined exhibited this particular characteristic. These SMSs, disseminated by fraudsters, contained words joined together without interceding spaces, rendering laborious comprehension. It is probable that fraudsters employ this tactic deliberately to deceive inattentive readers, as suggested by Luck (2007). Confounded recipients may unwittingly succumb to these deceitful schemes. Individuals receiving such texts should exercise caution and refrain from making hasty decisions that may ensnare them. Presented below is an example of such SMSs.

kumiliki Mari bira kafar.kupata kazi.masomo.kumrudisha mke mme.nyota,kesi.uzazi.biashara.pete.kama unashida piga (0689037067)
owning wealth without sacrifice.getting a job.studies.bringing back the husband.horoscope,case.birth.business.ring.if you have problems call (0689037067)

Spelling mistakes: Spelling errors are not uncommon in written communication; however, frequent occurrences may raise suspicions. Among the typographical errors observed in the collected data was the misspelling of several words, potentially distorting the intended meaning, as it argued by Peters (2013). Such distortions could lead recipients to inadvertently respond to the SMS in a manner favourable to fraudsters. The subsequent SMS serves as an example of this phenomenon.

iyo ela itume sasa hivi kwa namba hii ya ttcl 07302808 jina lije (AMINA TEBE)
send that money right now to this ttcl number 07302808 the name will come (AMINA TEBE)

Therefore, upon receiving an SMS resembling the one presented, individuals should exercise caution to mitigate the risk of falling prey to fraudulent schemes.

Writing entirely in uppercase: This is another notable feature observed in the gathered SMSs. Although it may be perceived as an attempt to emphasise the message, this writing style typically raises suspicions, casting doubt on the intended meaning of such SMSs. Such instances were particularly prevalent in SMSs related to superstition, rental and landlords, as well as those urging recipients to join secretive organizations (specifically referencing Freemasonry). Consider the following SMS as an illustration:

ASALAAM ALEYKUM BABU NIMESHARUDI NAKUOMBA KESHO ASUBUHI NJOO NA UDI 4 CHUMVI YA MAWE CENT YA ZAMANI MVUTO NA MCHANGA WAKAZINI KWAKO NIJE NIMALIZE SHIDA YAKO
ASSALAAM ALEYKUM GRANDSON/GRANDAUGHTER I ASK YOU TOMORROW MORNING TO COME WITH INCENSE 4 SALT OLD CENT ATTRACTION AND SAND FROM YOUR WORKPLACE LET ME COME AND END YOUR PROBLEM

As asserted by Chaka (2015) and Linden (2020), writing in all capital letters is commonly perceived as impolite and may be interpreted as shouting at the recipients of the message. Such formatting can cause skepticism regarding the authenticity of the SMS. Hence, it is imperative to invest time in verifying the authenticity of SMSs written in this manner.

Ignoring or misplacing punctuation: In written communication, punctuation plays several pivotal roles. Proper punctuation enhances text readability, clarifies meaning, and aids in text comprehension (Chen, Huang, & Ye, 2017). However, in the fraudulent SMSs studied, numerous punctuation errors were noted. These included misuses of question marks, commas, and periods. It is plausible that the fraudsters, as senders of these SMSs, intentionally wrote them (SMSs) with such errors to obscure the SMSs, thereby confusing recipients. Confused recipients are susceptible to falling victim to scams. This characteristic was particularly prevalent in SMSs concerning money transfers. The following SMS serves as an example of this phenomenon:

Yule babu kutoka sumbawang mganga namba yake ni iyo 0714665777)anasaidia kupata mali,kuludisha mke au mume ,magonjwa mbali mbali ,kipaji,masomo,biashara
The old man from Sumbawanga the healer his number is 0714665777) he helps to get wealth, to bring back a wife or husband, various diseases, talent, studies, business

This writing style causes challenges to readers, particularly those with visual impairments, in comprehending the text. Therefore, individuals encountering messages of this nature should exercise precautionary measures before taking any decision.

Distinctive writing styles

The fraudulent SMSs under study exhibited distinctive writing patterns, particularly those designed to persuade recipients into transferring money. Notably, these SMSs directed recipients to transfer funds to a number different from the one from which the SMS originated, a consistent pattern observed across all SMSs with fraudulent intent. Furthermore, the purported recipients' names were predominantly written in uppercase letters, likely a deliberate tactic to prevent funds from being transferred to unintended number. The prevalence of such uniform writing patterns suggests a concerted effort by a small group of individuals or a network collaborating to orchestrate these fraudulent activities. Consider the following example:

Ela itume kwenye AirtelMoney hii No.0786833994 Jina litakuja KALISTA TRIFONI MWANAHIYA
Please send that money to AirtelMoney No. 0786833994 The name will come KALISTA TRIFONI MWANAHIYA

Likewise, there is a noteworthy pattern concerning the mobile companies utilised for fraudulent money transfers. The study findings indicate a significant prevalence of fraudulent SMSs involving Airtel, tempting recipients to transfer money, the findings which are congruent to the Tanzania Communications Regulatory Authority's (2023, p. 49) report. This entails that fraudsters may have identified security susceptibilities within this particular telecommunications operator, enabling them to execute their schemes covertly and without detection.

Another notable pattern that emerges is the substantial proportion of female names (84%) associated with the recipients of transferred funds. This indicates a significant increase in the utilisation of mobile networks for deceptive purposes by women. This trend is frequently observed in fraudulent SMSs pertaining to money transfers. These findings are consistent with those of the 2003 Australian census, which revealed that among 812 prisoners whose primary offense involved fraud and deception, 21% were female, constituting 11% of the total female prison population, while only 3% of male prisoners were incarcerated for similar offenses (Goldstraw, Smith & Sakurai, 2005). This implies that contrary to the conventional notion that fraudsters are predominantly male, fraud constitutes a notable aspect of female criminal behavior. Furthermore, in addition to delineating motives for fraudulent activities, women are also implicated in more elaborate and meticulously planned instances of serious fraud.

Deficiency of politeness markers

Politeness constitutes a fundamental element of effective communication. As it regulates cooperative behavior in discourse, politeness significantly influences interactions (Thomas, 1995). One aspect of polite communication entails the use of language that demonstrates respect for the recipient, such as the inclusion of "please" (Fraser, 1996; House, 1989; Sato, 2008; Wichmann, 2005), particularly when making requests for

assistance or services to which one is entitled. Regrettably, this feature was notably absent in the majority of fraudulent SMSs, with only one SMS adhering to this norm. The prevalence of imperative language in the majority of SMSs impedes effective communication. This feature is demonstrated in the following SMS.

nitumie kwenye namba ya vodavom hii 0763458839 jina OSCAR MAVUNJE
send me (the money) on this vodavom number 0763458839 name OSCAR MAVUNJE

Consequently, it becomes imperative to scrutinise both the source and intent of a message should one encounter an SMS characterised by this particular feature.

Easy money-making promises

Among the fraudulent SMSs analysed, a subset contained enticing promises of rapid wealth attainment with minimal effort. Alarmingly, these SMSs failed to elucidate the mechanisms through which recipients would amass such wealth. They appeared to be deceptive tricks orchestrated by imposters posing as magicians or agents of organisations like the Freemasons. The latter, posing as Freemason agents, coax recipients into joining their association under the guise of achieving wealth. Many people, succumbed by financial hardship and the allure of quick riches, fall prey to these traps and subsequently become ensnared by fraudsters. If the senders of these SMSs truly have the ability to make people wealthy, they would not solicit money from recipients of their SMSs; rather, they would employ their purported abilities to generate wealth for themselves. It is, thus, crucial for people receiving such SMSs to exercise utmost caution to avoid victimisation by these fraudsters. Below is an example of such an SMS.

JIUNGE FRIMASON UWEZE KUMILIKI PESA MAJUMBA NA MAGARI YA KIFAHARI KUKUZA BIASHARA,VIPAJI PIGA NAMBA 0733584411 KAMA UKO TAYARI KUJIUNGA
JOIN FREEMASON YOU TO OWN MONEY HOUSES AND LUXURIOUS CARS TO DEVELOP BUSINESS, TALENTS CALL 0733584411 IF YOU ARE READY TO JOIN

Social problems-solving promises

In fraudulent SMSs, fraudsters not only claim to be capable of offering solutions to economic hardships but also claim to possess magical abilities to address a wide range of social problems. These include driving away evil spirits, providing employment opportunities to the unemployed, predicting results in betting activities, reuniting estranged spouses, and addressing numerous other societal challenges of similar nature. Such SMSs serve as bait for people grappling with such challenges. Exploiting the knowledge that many people encounter similar difficulties and are susceptible to such enticing promises, fraudsters use this susceptibility to victimise unwary individuals. These SMSs are frequently disseminated by individuals posing as magicians, who promise to possess mystical powers capable of alleviating various societal difficulties. An example of such an SMS is provided below.

Mpigie mzee watiba asilia anatibu magonjwa mbalimbali machimboni,masomoni,zindiko pete ya bahati,kuludisha mke&mume, mifugo kuibiwa,mali bilakafala cheo, N.k piga sim (0715661252)
Call an old traditional healer he heals various diseases in the mines, in the studies, fortification charm, lucky ring, bringing back a wife and husband, stolen livestock, property without sacrifice, promotion etc. call (0715661252)

In this particular case, the sender presents themselves as a witch doctor, claiming to possess the capability to address a multitude of socioeconomic challenges. Such tactics exemplify the strategies employed by these fraudsters in their deceitful endeavours.

Extorting

A subset of SMSs exhibits characteristics suggestive of extortion. These SMSs threaten recipients by alleging that they have received assistance from individuals posing as witch doctors or magicians in amassing wealth, yet have failed to reciprocate this assistance. These SMSs, originating from cybercriminals, aim to defraud unwary recipients. It is imperative for individuals to recognise and be vigilant against such SMSs to prevent falling into the traps set by these malicious actors. Below is an example of such an SMS.

super feo nasikitika sana nimekupa ndangu na umefuata masheriti na umepata utajili mkubwa na unaniheshimu babu yako ukumbuke wewe na wenzako mwendamseke manyanya na huyu chijana wa Mwanza nimemusaidia ila kwa

heshima yako nimemusaidia amefanikiwa hataki kuja kushukuru ananitumia pesa tu mwambie asione magari yake na nyumba alizojenga kafika anaweza baki bila kitu na wewe badilisha dawa kwenye mabasi yote patakuku mweusi uchinje damu mwagia katika mto wamaj
super feo, I am very sorry that I gave you my charm and you have followed the rules and you have become prosperous and you respect me, your witch doctor, remember that you and your colleagues mwendamseke manyanya and this young man from Mwanza, I have helped him just to respect you, I have helped him he is now successful but he does not want to come to thank me; he is just sending me money; tell him I have power to dispossess him with everything he owns. And you change the charm for your buses; slaughter the black chicken and pour its blood in the river

Hide the purpose of the money transfer

Fraudulent SMSs often exhibit this characteristic, especially in SMSs luring money transfers. Legitimate SMSs from credible sources typically specify the amount of money to be transferred and provide a clear purpose for the transaction. However, in the examined fraudulent SMSs, neither the transfer amount nor its intended purpose was specified. This deliberate omission aims to confuse and deceive recipients, particularly those who may have previously promised to transfer money. Therefore, individuals receiving SMSs with this feature must exercise caution to evade falling into the traps set by these fraudsters.

Impersonation

Another prevalent feature observed in fraudulent SMSs collected is impersonation, defined as the act of deceiving someone by assuming the identity of another individual (Banerjee, Barman, Faloutsos, & Bhuyan, 2008; Gharawi et al., 2021). This feature is particularly prominent in fraudulent SMSs that coax recipients into sending money to purported landlords, where the fraudsters impersonate the landlords. SMSs incorporating this feature obfuscate the identity of the impersonator, mirroring the approach seen in other fraudulent activities (Beju & Făt, 2023; Bidgoli & Grossklags, 2017; Bruno, 2019; Mansfield-Devine, 2016; Smith, 2013). The deliberate anonymity of the sender facilitates the deception and potential victimisation of SMS recipients. The perpetrators are cognizant that some recipients may be tenants who may have outstanding rent payments, rendering them susceptible to their schemes. An example of such an SMS is provided in the following passage.

Nitumie kwenye airtelmoney kwa namba hii 0788693319 unapotuma jina litakuja EDITHA MAKUMI
Send me (the money) on airtelmoney at this number 0788693319 when you send the name will come EDITHA MAKUMI

Upon reading this SMS, one would be inclined to believe that the sender of such an SMS is the real landlord. However, the reality is that these SMSs are sent by fraudsters masquerading as landlords. Hence, individuals must exercise caution when receiving such SMSs to mitigate the risk of falling prey to these fraudulent schemes.

6. Contribution of the study

The present study contributes to providing an understanding of the various mechanisms employed by fraudsters in their use of SMS to defraud people. This is made possible by examining and identifying the forms and features of fraudulent SMS presented in the study. Understanding the forms and features of these SMSs provide important insights into the linguistic and stylistic patterns contained in such SMSs. Therefore, this research gives the recipients of these SMSs an understanding that enables them to take important precautions and make the right decision when they receive such SMSs. By doing so, recipients are more likely to be able to protect themselves and others against such fraudulent schemes.

7. The implications of the study

The implications of this study covers several aspects which are outlined as follows:

Heightening awareness

One of the main implications of the current study is to heighten people's awareness of the existence of the cybercrime committed through fraudulent SMS. It is likely that some people were receiving these messages unaware that they were crafted for crime purposes. This study will awake sleepy people and educate them to

be watchful with such messages. This awareness is important as it will help save people from cybercrime through SMSs.

Providing risk reduction techniques

The present study will enable the recipients of the fraudulent SMSs to recognise them (SMSs) and thus protect themselves against the tricks of these fraudsters. This is due to the fact that this study identifies the types of fraudulent SMS and their features. Identifying those forms and the contained features is an important step in reducing the possibility of getting into the fraudsters' traps.

Stimulating policy and legal reforms

The results of this study can stimulate improvements to inform policy makers and regulators about the need for more effective measures to combat fraudulent practices committed through SMS. This may involve the improvement of laws for the protection of mobile users, strengthening the security systems by mobile operators, or improving policies related to communication matters to ensure that mobile users, especially those using the short message service (SMS) do not fall into the hands of fraudsters.

8. Conclusion and recommendations

The main objective of the current study was to uncover the cybercrime tactics by studying the emerging features and forms of fraudulent SMS, especially those distributed by fraudsters to "innocent" Tanzanians. The motivation to conduct such a study was due to the existence of many cybercrime incidents involving the use of SMS, thus leading to several people being tricked and defrauded by these fraudsters. Although it is not easy to know the exact number of people who have been deceived by these fraudsters, it is obvious that a large number of people have already encountered this kind of fraud. In this study, various forms of fraudulent SMS have been identified, including those involving money transfers, superstitions, rental and landlords, false lottery, easy-money-making, extortion, and false employment offers. The study reveals that fraudulent SMSs persuading recipients to send money to the senders (fraudsters) were the most prevalent, followed closely by SMSs with superstitious content. This indicates the high efficiency of these two forms of SMSs in facilitating fraudulent activities, thus requiring great attention among the recipients of such SMSs to reduce the risk of being scammed. On the contrary, fraudulent SMSs related to false employment offers were not much preferred by fraudsters; this is probably due to their low efficiency in carrying out such schemes. However, recipients should not ignore SMSs of this nature; taking precautions should be the most important thing when anyone comes across any SMS with fraud indicators. To prevent cybercrime via SMS, recipients must refrain from engaging in or disclosing any sensitive information by responding to such messages. Furthermore, this study identified several features found in fraudulent SMS that were involved in this study. Such features include the absence of formal salutations, anonymity of the sender and recipient, typographical errors, distinctive writing styles, and the deficiency of politeness markers. Easy money-making promises, social problem-solving promises, extorting, hiding the purpose of the money transfer, and impersonation were other observed features. Recipients who come across SMSs that contain these attributes should be extra careful to avoid falling prey to the illegal tactics of these scammers. This study serves as an important tool to alert people who are susceptible to these fraudulent schemes to fight and stop this crime.

The present study recommends that SMS recipients should be careful and spend enough time evaluating the SMS they are worried about in order to test their genuineness before taking decisions or following the instructions contained in those SMSs. Considering the prevalence of fraudulent SMS, recipients should be careful, especially about messages that direct them to send money without stating why they should do so. Also, the recipients of these SMSs should be careful when they receive an SMS that makes sweet promises such as solving some societal challenges. Those with various social predicaments should remember that there is not always a shortcut and quick way to deal with the challenges they might have. They should remember the Swahili saying, "Haraka haraka haina baraka" (Haste makes waste). Therefore, the recipients of these SMSs can minimize the possibility of being scammed if they do a detailed evaluation of the SMS they receive to satisfy themselves if the SMS is genuine or not. Additionally, recipients are advised to report suspected fraudulent SMS to relevant authorities or regulatory agencies (in Tanzania we have TCRA "Tanzania Communications Regulatory Authority"). This may help to disrupt the malicious plans of these fraudsters, but it also helps to identify those responsible for these schemes. Should this be successful, it will contribute to shielding the entire community against these kinds of practices that harm both individuals and the country

at large. This study also recommends educating the public about the existence of this kind of fraud. This may go hand in hand with educating the community regarding the various mechanisms used by these cybercriminals in carrying out fraud through SMSs. Awareness campaigns and educational programs will play an important role in enabling people to identify the indicators of SMS with fraudulent content, thus enabling the community to deal with this form of fraud. Furthermore, this study calls for mobile network operators to strengthen their security systems, especially during mobile number registration. As this study shows, one mobile phone operator was responsible for 68.7 percent of all fraudulent SMSs collected. This indicates the presence of security loopholes in the particular mobile operator, which triggers the need to further strengthen the security systems on mobile networks to protect their customers against the possibility of fraud.

9. Funding

This study received no internal or external funding.

ORCID

Lazaro Charles https://orcid.org/0009-0004-7391-2454

References

1. Ajayi, T. M. (2022). Discursive-manipulative strategies in scam emails and SMS: The Nigerian perspective. *Lodz Papers in Pragmatics*, *18*(1), 175-195.
2. Akbar, N. (2014). *Analysing persuasion principles in phishing emails.* Master's thesis, University of Twente.
3. Akindele, D.F, 2007. Lumela/Lumela: A socio-pragmatic analysis of Sesotho greetings. *Nordic Journal of African Studies, 16*(1), 1–17
4. Alake, T. O. (2017). Pragma-stylistic analysis of selected Nigeria electronic advanced fee fraud texts. *Southern Semiotic Review*, *8*(1), 97-113.
5. Ayeomoni, N. (2003). *The role of stylistics in literary studies*. Ile-Ife: Obafemi Awolowo University Press.
6. Banerjee, A., Barman, D., Faloutsos, M., & Bhuyan, L. N. (2008, April). Cyber-fraud is one typo away. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications* (pp. 1939-1947). IEEE.
7. Beju, D. G., & Făt, C. M. (2023). Frauds in banking system: Frauds with cards and their associated services. In *Economic and Financial Crime, Sustainability and Good Governance* (pp. 31-52). Cham: Springer International Publishing.
8. Bidgoli, M., & Grossklags, J. (2017, April). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. In *2017 APWG Symposium on Electronic Crime Research* (eCrime) (pp. 57-69). IEEE.
9. Brown, S. (2005). *Telecommunication fraud management*. Waveroad Securit.
10. Brown, W., & Reynolds, M. (1975). A model of IQ, occupation and earnings. *American Economic Review, 65*, 1002−1007.
11. Bruno, M. (2019). Impersonation fraud scenarios: How to protect, detect and respond. Cyber Security: *A Peer-Reviewed Journal, 3*(1), 6-13.
12. Çakar-Mengü, S., & Mengü, M. (2023). Cyberbullying as a manifestation of violence on social media. *Multidisciplinary Perspectives In Educational And Social Sciences Vi*, 47.
13. Chaka, C. (2015). Textisms, grammatical features, and sentence types in the SMS and IM paragraphs of EFAL learners. *Per Linguam: A Journal of Language Learning Per Linguam: Tydskrif vir Taalaanleer*, *31*(3), 65-85.
14. Chapman, S., & Clark, B. (2014). Introduction: Pragmatic literary stylistics. In *Pragmatic Literary Stylistics* (pp. 1-15). London: Palgrave Macmillan UK.
15. Chen, X., Huang, B., & Ye, D. (2017). *The role of punctuation in P2P lending: Evidence from the People's Republic of China. ADBI Working Paper 787*. Tokyo: Asian Development Bank Institute. Available: https://www.adb.org/publications/role-punctuation-p2p-lending?evidence-prc
16. Chete, F.O, Oyemade, D., Abere, R., Chiemeke, S.C., & Ima-Omasogie, I. (2012). Citizens' adoption of SMS based on E-Government Services in Lagos state, Nigeria. *Journal of Emerging Trends in Computing and Information Sciences, 3*(4), 654-660.
17. Crews, C. W. (2007). Cybersecurity and authentication: The marketplace role in rethinking anonymity-before regulators intervene. *Knowledge Technology Policy, 20*,97-105.

18. Duha, N. (2021). Short message services (SMS) fraud against mobile telephone provider consumer review from law number 8 of 1999 concerning consumer protection. *Journal of Law Science, 3*(1), 36-43.

19. Dzameshie, A. K. (2002). The forms, functions and social value of greetings among the Ewes. *New directions in Ghanaian linguistics*, 381-408.

20. Faluyi, B., Fele, T., & Ayemi, A. (2020). Impact of ICT-facilitated fraud on sustainable socio-economic development in Nigeria. *Journal of Education and Social Development*, 23-27.

21. Fowler, R. (1986). *Linguistic criticism*. London: OUP.

22. Fraser, B. (1996). Pragmatic markers. *Pragmatics, 6*(2), 167-190.

23. Gharawi, M. A., Badawy, A., Ramadan, D. E., & Elsayed, S. (2021). Social media impersonation in the virtual world. *Al-Hikmah: International Journal of Islamic Studies and Human Sciences, 4*(1), 57-65.

24. Goldstraw, J., Smith, R. G., & Sakurai, Y. (2005). *Gender and serious fraud in Australia and New Zealand*. Canberra: Australian Institute of Criminology.

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

26. House, J. (1989). Politeness in English and German: The function of please and bitte. In S. Blum-Kulka, J. House, and G. Kasper (eds.). *Cross-cultural pragmatics: Requests and apologies* (pp. 123-155). Norwood, NJ: Ablex.

27. Leech, G. N. (1969). *A linguistic guide to English poetry*. London: Longman.

28. Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction (TOCHI), 26*(5), 1-28.

29. Linden, J. (2020). Contrastive focus capitalization: Nonstandard usages of capital letters in web-based English and their capital-I implications. *Studies in the Linguistic Sciences: Illinois Working Papers*, 116-138.

30. Liu, M., Zhang, Y., Liu, B., Li, Z., Duan, H., & Sun, D. (2021, December). Detecting and characterizing SMS spearphishing attacks. In *Proceedings of the 37th Annual Computer Security Applications Conference* (pp. 930-943).

31. Luck, G. (2007*). Conjectural emendation in the Greek New Testament*, 169-202

32. Lyons, C. (2019). *Cyber-enabled financial abuse of older Americans: A public policy problem*. PhD dissertation, University of Baltimore.

33. Mansfield-Devine, S. (2016). The imitation game: How business email compromise scams are robbing organisations. *Computer Fraud and Security, 2016*(11), 5-10.

34. Mat-Dangi, M. R., & Tajuddin, N. (2013). Fraud responses through short text messages (SMS): A qualitative study on enthusiasm, power of influences and impacts to the university students. *KONAKA*, 392-404.

35. Maurya, S. K. (2023). Nature, forms, and remedies of cyberbullying on social media platforms: A brief philosophical perspective. In *Cybersecurity for Decision Makers* (pp. 29-43). CRC Press.

36. National Fraud Authority. (2014). *Annual fraud indicator, June 2013, 2014.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/.

37. Nlebedum, C. (2017). *Dear valued customer: A forensic-linguistic analysis of scam texts*. M.A thesis, University of Lagos.

38. Onanuga, P. (2017). Language use in Nigerian spam SMSs: A Linguistic Stylistic Analysis. *Language Matters, 48*(2), 91-116.

39. Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies, 128*, 17-26.

40. Pervaiz, F., Nawaz, R. S., Ramzan, M. U., Usmani, M. Z., Mare, S., Heimerl, K., ... & Razaq, L. (2019, July). An assessment of SMS fraud in Pakistan. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies* (pp. 195-205).

41. Peters, M. L. (2013). Spelling caught or taught: A new look. London: Routledge & Kegan Paul plc.

42. Rose-Ackerman, S. (2010). The law and economics of bribery and extortion. *Annual Review of Law and Social Science, 6*, 217-238.

43. Sato, S. (2008). Use of 'please' in American and New Zealand English. *Journal of Pragmatics, 40*(7), 1249-1278

44. Scott, C. R. (2004). Benefits and drawbacks of anonymous online communication: Legal challenges and communicative recommendations. In S. Drucker (Ed.), *Free speech yearbook* (Vol. 41, pp. 127-141). Washington, DC: National Communication Association

45. Slaney, P. (2024, July 7). *How SMS scams threaten your business*. https://www.linkedin.com/pulse/how-sms-

scams-threaten-your-business-paul-slaney-na1qe/#:~:text=How%20SMS%20Scams%20Threaten%20Your%20Business

46. Smith, R. G. (2013). Identity theft and fraud. In *Handbook of internet crime* (pp. 273-301). Willan.

47. Strauss, A. L., & Corbin, J. M. (1990). Basics of qualitative research (Vol. 15). Newbury Park, CA: Sage.

48. Tanzania Communications Regulatory Authority. (2023). *Communication statistics: Quarter ending 30th June 2023.* https://www.tcra.go.tz/uploads/text-editor/files/Communication%20Statistics%20for%20Q4%202023_1689695039.pdf

49. Thomas, J. (1995). *Meaning in interaction*. New York: Longman.

50. Thorne, J. P. (1965). Stylistics and generative grammars. *Journal of Linguistics, 1*, 49-59.

51. Ugwu, C. N., & Eze, V. H. U. (2023). Qualitative research. *IDOSR Journal of Computer and Applied Sciences, 8*(1), 20-35.

52. Wachtel, P. (1976). The effect on earnings of school and college investment expenditures. *The Review of Economics and Statistics, 58*(3), 326–331.

53. Wichmann, A. (2005). Please —from courtesy to appeal: The role of intonation in the expression of attitudinal meaning. *English Language and Linguistics, 9*(2): 229-253.

54. Zubair, M., Zubair, S., & Ahmed, M. (2023). Cyberbullying instilled in social media. In *Cybersecurity for Smart Cities: Practices and Challenges* (pp. 17-29). Cham: Springer International Publishing.