ISSN : 2350-0743

*International Journal of Recent Advances in Multidisciplinary Research*

*Vol. 12, Issue 06, pp.11379-11387, June, 2025*

## RESEARCH ARTICLE

# ANALYZING POWER THROUGH LANGUAGE IN SPAM EMAILS: A CRITICAL DISCOURSE APPROACH

***Batool Dahham Al Ali**

Departemnt of Oil and Gas, Basra University for Oil and Gas Engineering, Iraq

## ARTICLE INFO

***Article History***

Received 20th March, 2025
Received in revised form
17th April, 2025
Accepted 16th May, 2025
Published online 30th June, 2025

***Keywords:***

Spam emails, Halliday's SFL Theory, Linguistic Features, Deception.

****Corresponding author:***
***Batool Dahham Al Ali***

## ABSTRACT

This study aims to investigate how language functions as a tool of deception within spam emails. The research involves a detailed analysis of the linguistic content found in 20 spam messages, focusing on the identification and examination of the linguistic features utilized. Particular attention is given to lexical, grammatical, and orthographic elements that spammers employ in crafting deceptive messages. The analysis is grounded in Halliday's Systemic Functional Linguistics (SFL) theory, particularly through the lens of the tristratal model, which guides the examination of various linguistic levels. Furthermore, the study explores how these linguistic choices contribute to manipulation and deceit. The findings reveal that spammers make deliberate and strategic linguistic choices designed to influence recipients' perceptions and prompt compliance. The analysis also underscores the importance of the linguistic options selected over other possible alternatives. Ultimately, the study concludes that these language strategies are intentionally designed to fulfill the spammers' goal—exploiting internet users, thereby contributing to the broader issue of cybercrime.

***Citation: Batool Dahham Al Ali. 2025.*** *"*Analyzing Power Through Language in Spam Emails: A Critical Discourse Approach..". *International Journal of Recent Advances in Multidisciplinary Research,* 12, (06), 11379-11387.

# INTRODUCTION

The rapid development of digital communication technologies has led to a surge in the use and relevance of electronic messaging, especially on platforms involving computer-mediated interaction. Although this form of communication is highly efficient, it also introduces significant risks due to its often vague and misleading content—spam emails being a prime example. These unsolicited messages, enabled by the anonymity of the internet, offer an ideal environment for cybercriminals to manipulate users through persuasive and deceptive language. Spam emails—whether posing as lottery wins or job opportunities—go beyond being simple annoyances; they function as vehicles for cybercrimes such as phishing. Spammers employ strategic language to manipulate their targets by triggering emotions like fear, urgency, or compassion. This manipulation relies on deliberate word choices that disguise malicious intentions behind what appears to be legitimate communication. According to (1), manipulation is a linguistic act designed to influence others while concealing the true intention behind the message. Its success hinges on both the linguistic tools used and the spammer's ability to hide their deceptive aims. As such, spam emails exemplify the use of language as a covert tool for deception, often going unnoticed by those who receive them.

**Statement of the Problem:** Although spam and phishing have a broad and harmful influence, most existing studies have prioritized technical defenses and legal approaches. The linguistic and rhetorical techniques found within spam emails have received minimal academic attention. As (2) observe, few investigations explore the deeper elements of spam messages, such as their language use, structure, and stylistic choices, beyond simply classifying them. This study aims to bridge that gap by exploring how spammers use language to deceive their targets. The effectiveness of spam is rooted not in complex cyberattacks but in the deliberate manipulation of words to shape behavior and extract personal data. Identifying these linguistic tactics is essential for understanding the role of language in online fraud and for better safeguarding individuals against such deceptive practices.

**Purpose of the Study:** This study primarily seeks to examine and interpret the linguistic elements utilized in spam emails to carry out deception. It focuses on how these language features are designed to provoke emotional reactions and prompt recipients to take actions that ultimately serve the interests of the spammer. Furthermore, the research emphasizes the significant role language plays in cybercrimes, demonstrating how fraudulent activities are carried out through skillful textual manipulation masked as persuasive communication. By analyzing various categories of spam emails, the study aims to show how language is strategically adapted to support the spammer's misleading intentions. In addition, the study offers valuable insights to both the fields of linguistics and cybersecurity by connecting language analysis with real-world applications in digital protection. It aims to enhance awareness of the manipulative use of language in online spaces and support the development of effective measures to combat cybercrime.

**Significance of the Study:** This study plays a crucial role in addressing the lack of academic focus on the linguistic aspects of spam emails. By analyzing the actual wording and structure used by spammers, it highlights how linguistic knowledge can be applied to better understand and combat online deception.

It also aims to raise public awareness by helping people identify manipulative language and reduce their risk of falling victim to spam-related scams. A key feature of the study is its use of Halliday's Systemic Functional Linguistics (SFL), which introduces an innovative approach and extends linguistic research into the realm of digital communication.

The outcomes of this research are relevant to both educational and technological sectors, providing a valuable linguistic perspective for detecting and preventing cyber fraud.

**Research Questions**

- What kinds of language elements are used in the content of spam emails?
- In what ways do these language elements serve to deceive and manipulate recipients?

**Definition of Key Terms**

□**Deception**: The intentional act of misleading others by providing false or distorted information, often involving hidden motives and manipulative tactics (3).

□**Spam**: Unwanted and often deceptive electronic messages, usually intended to scam or trick recipients through methods like phishing (4).

□**Phishing**: A form of spam specifically designed to fraudulently obtain confidential personal or financial data from individuals through misleading communication (5).

□**Linguistic Manipulation**: The calculated use of language to distort reality and mislead recipients, aiming to sway their thoughts or actions (1).

□**Online Anonymity**: The concealment of a sender's identity in digital communication, often used to mask intent and facilitate deceptive practices (6)

# LITERATURE REVIEW

With the widespread use of the internet, online communication has become increasingly exposed to cyber threats, particularly spam and phishing attacks. According to researchers like (7)(2), spam refers to unsolicited emails, often sent in large quantities for either promotional or fraudulent purposes. These messages commonly use manipulative language to deceive recipients, extract personal data, and cause both emotional and financial damage. A well-known example is the "Nigerian 419" scam, which showcases how language and psychological tactics have long been used to commit fraud and have evolved alongside technological advancements (8). Beyond individual victims, spam presents broader economic risks. For example, (9) reported major financial losses due to spam as early as 2005, underscoring the importance of addressing this issue. Spam emails often include traits like commercial motivations, mass distribution, and emotional manipulation that disrupt everyday communication (10). Phishing, a subtype of spam that began in the 1990s, involves deceiving individuals into disclosing private information. Like spam, its primary goals include stealing identities and accessing confidential data (11). Phishers often imitate trustworthy organizations, using convincing visuals such as logos and legal documents to appear legitimate (2). (12) outlines several categories of email—including newsletters, promotional content, surveys, transactional emails, announcements, and plain text—each with specific functions in online interaction. While email remains a vital communication tool, its openness makes it susceptible to manipulation and fraud (13). This section underscores how language plays a key role in these deceptive practices and introduces Halliday's Systemic Functional Linguistics (SFL) as a useful model for examining the linguistic features found in spam messages.

**Categories of Spam Emails and Their Deceptive Techniques:** Spam emails are a type of cybercrime where fraudsters use deception to steal personal data and money. (14) emphasize that the anonymity of online platforms facilitates such scams. (15) categorizes spam into seven main types: (1) Dormant Account scams, where spammers claim access to inactive bank accounts and seek the recipient's confidential assistance (4) ; (2) Charity scams that exploit emotional or religious appeals to solicit donations; (3) Lottery Win scams that falsely inform recipients of winnings to extract sensitive information; (4) Business Transaction scams that lure victims into sharing documents for fake investments; (5) Rescue Operation scams featuring fabricated emergencies to request money transfers; (6) Shopping spam promising free gifts in exchange for personal data; and (7) Account Update scams that trick users into revealing credentials under the guise of system updates. Deception, as described by (3), involves manipulating people into believing falsehoods. Spammers utilize complex psychological and linguistic tactics (5), such as creating urgency, appealing to emotions, and building trust. (16) notes these emails often include intentional grammatical mistakes and emotionally charged language designed to distract and gain victims' confidence. According to (15), spammers are typically skilled psychologically and linguistically, employing personalization and presuppositions to make their messages feel individualized. (17) and (18) add that captivating subject lines and structured messaging enhance the likelihood of engagement. Overall, spammers combine technical, psychological, and linguistic methods to deceive and manipulate recipients.

This literature review examines the deceptive methods employed in spam emails, highlighting how linguistic manipulation enables scammers to mislead targets. (4) points out that spammers craft themed messages that conceal their true intentions. They often impersonate affluent, educated individuals to build credibility and emotional rapport, aiding their fraudulent schemes. As online deception grows, its detection becomes more challenging. Unlike face-to-face fraud, electronic deception benefits from anonymity, with analysts relying solely on message content to detect dishonesty (19). The Text-Based Approach, which analyzes linguistic and textual features, is a key method in uncovering deception. Scholars like (20) and (21) observe that spammers vary in genre, formality, and language tactics. Tools such as Discourse Analysis, Criteria-Based Content Analysis (CBCA), and

Reality Monitoring (RM) help reveal deceitful intentions. (22) identify typical spam characteristics including low informativeness, deliberate grammatical and spelling errors, and restrained expressiveness—strategies used to control the message and maintain the illusion of authenticity (23) and (4) highlight that spammers intentionally use emotionally persuasive language to build trust. (13) describe a multi-stage process in spamming:

- Solicitation – gaining trust and offering rewards.
- Formal Extraction – initiating theft after trust is established.
- Irritation – applying pressure if the victim resists.
- Personal Appeal – reinforcing emotional or personal credibility.

These tactics demonstrate that although spammers may not always use perfect grammar, they are highly adept at manipulating tone, style, and content to evoke feelings like fear, sympathy, and urgency. Consequently, analyzing textual and linguistic features is crucial for detecting fraudulent intent.

**Language as a Tool of Influence and Manipulation:** According to (1), language functions as a powerful tool of manipulation, shaped by the speaker's intentions and the surrounding context. Manipulation can be either deliberate—when a speaker intentionally influences others—or unintentional. Spam emails are a clear example of deliberate manipulation, as spammers carefully design messages to deceive recipients. (6) and (24) emphasize that language plays a fundamental role in forming social interactions, often subtly guiding behavior and shaping perceptions. (1) further explains that manipulation uses techniques that exploit emotions and distort rational thinking, such as rhetorical tricks and misleading impressions, which encourage recipients to act in ways that benefit the sender, highlighting language as a key element in the manipulation process.

**Related Studies:** Several studies support the view that spam emails are highly sophisticated tools of manipulation. (25) discuss how spam has evolved from being a mere annoyance to a form of cybercrime, particularly through phishing schemes. (20) highlight the emotional effects of spam, such as provoking fear or anxiety. (18) observe that spam often pressures recipients to respond quickly, thereby avoiding careful, rational thinking. Research by (26), (27), and (28) examine the rhetorical and syntactic features of spam messages. For instance, spam frequently emphasizes subjects and verbs to convey urgency and authority. Additionally, the use of gendered language is noted, with emotional appeals targeted more towards female recipients and logical appeals directed at males (14). These findings demonstrate that spammers deliberately manipulate linguistic style and structure to sway recipients' choices.

**Theoretical Framework: Halliday's Systemic Functional Linguistics (SFL):** This study uses Halliday's Systemic Functional Linguistics (SFL) theory to analyze the language of spam. SFL views language as both a system, providing various linguistic options, and a tool that serves different communicative functions. According to (29), language operates through three metafunctions:

- Ideational: conveying ideas and experiences.
- Interpersonal: managing social interactions through mood and modality.
- Textual: structuring information in relation to context and theme.

(30) further elaborates that meaning is shaped by lexico-grammar and orthography. SFL highlights that language choices depend heavily on context, and that what is left unsaid can be as meaningful as what is expressed. (4) and (31) endorse using this framework to study spam, suggesting that detecting deception requires analyzing linguistic patterns within their specific contexts. In summary, the reviewed literature shows that spam emails employ intricate linguistic techniques to manipulate their recipients. Identifying deception depends on detailed linguistic analysis, and frameworks like SFL provide effective tools to uncover the subtle, strategic use of language in such cybercrimes.

# METHODOLOGY

The methodological framework for this study is designed to investigate the linguistic characteristics of spam emails and their role in deception through a qualitative approach based on Halliday's Systemic Functional Linguistics (SFL) theory. The framework is structured around several main elements: the corpus, research design, theoretical foundation, procedures, data collection and analysis, ethical considerations, and a concluding section that summarizes the overall methodology.

**Corpus Description:** The researcher assembled a corpus of 20 spam emails sourced from www.419scam.org, covering a variety of fraudulent types. These include lottery scams, charity appeals, job offers, business proposals, and dormant account notifications. This diverse selection was chosen to ensure content variety and reliability, enabling an examination of how language differs across various fraudulent scenarios. Each category of spam employs distinct deceptive tactics:

- Lottery scams falsely promise winnings.
- Charity emails use emotional appeals to solicit donations.
- Job and business offers request personal information under misleading pretenses.
- Dormant account scams offer fake monetary rewards in exchange for involvement.

The corpus serves to illustrate how spammers manipulate language to influence recipients, highlighting the linguistic strategies used in different forms of fraud. The emails vary in length and format, which supports the study's objective of identifying common and widespread linguistic patterns.

**Research Design:** The study employs a non-experimental, qualitative descriptive design, which aligns well with its goal of interpreting and analyzing linguistic data rather than measuring it quantitatively. As noted by researchers like (32), qualitative research is especially effective for investigating language phenomena that cannot be easily quantified. This approach enables a thorough, context-sensitive examination and interpretation of how language is used in spam emails. The researcher chose qualitative methods to reveal the meanings, intentions, and deceptive tactics within the texts—insights that quantitative or experimental methods cannot provide. This choice is supported by scholars such as (33),(33) and (34) who emphasize the importance of qualitative methods for gaining a deeper understanding of human communication.

**Chosen Framework: Systemic Functional Linguistics (SFL):** This study is guided by Halliday's Systemic Functional Linguistics (SFL) as its theoretical framework, selected for its suitability in analyzing both the linguistic and functional aspects of texts. SFL views language as systemic, focusing on the choices speakers make, and functional, highlighting the purposes those choices serve within a given context. This combination aligns closely with the study's aim to investigate how language is employed in spam emails and why particular linguistic features are chosen. SFL's three-tiered model provides a valuable approach, encompassing:

- Discourse-Semantics, which addresses language metafunctions:
    - Ideational (expressing content and ideas),
    - Interpersonal (engaging with the reader),
    - Textual (structuring and organizing the text).
- Lexico-Grammar, concerning the vocabulary and grammatical patterns selected.
- Phonology/Orthography, covering sound and writing systems, including formatting and emphasis.

By applying this framework, the researcher goes beyond merely identifying linguistic features to understanding the deliberate choices made, revealing the underlying manipulative tactics in spam discourse.

**Procedure of the Study:** The research commenced with the compilation of data, where the researcher selected 20 spam emails representing various types of scams. These samples were chosen to ensure diversity and to capture a wide range of linguistic features and deceptive methods. The analysis was conducted using the SFL framework, with the researcher closely examining the lexical choices, grammatical patterns, and discursive techniques in each email. The focus was on how these elements work together to facilitate manipulation and deception. The study centered on the three metafunctions of language:

- The ideational metafunction, which uncovers the content and messages conveyed.
- The interpersonal metafunction, which explores how the writer interacts with and influences the reader.
- The textual metafunction, which reveals how the information is organized to enhance clarity and persuasion.

Through this interpretive and functional approach, the researcher was able to link specific linguistic features to manipulative tactics such as impersonation, emotional appeals, and creating a sense of urgency.

**Data Collection and Analysis:** Data collection was carried out through purposive sampling from www.419scam.org, selecting a well-rounded and representative set of spam emails. The variety of spam types enhanced the study's validity and provided a comprehensive foundation for analysis. For the data analysis, the researcher employed the SFL framework across all three levels—semantic, grammatical, and orthographic—to investigate how spammers manipulate language to deceive recipients. The analysis uncovered recurring patterns in vocabulary, modality, the use of personal pronouns, and text structure that serve to build trust, generate urgency, or mimic authority. This qualitative and interpretive method enabled the researcher to reveal the hidden role of language in online fraud and connect these linguistic tactics to wider cybercrime strategies.

**Examination and Interpretation of Linguistic Characteristics in Spam Emails:** This section provides an in-depth analysis of the language used in spam emails, highlighting how linguistic strategies are deliberately employed to manipulate and deceive recipients. The study explores the specific linguistic features found in these messages using Halliday's Systemic Functional Linguistics (SFL) framework, with particular emphasis on its three-layered model, which examines lexico-grammar and orthographic aspects. The analysis addresses research questions concerning the kinds of linguistic elements present and their roles within the context of cybercrime and the victimization process.

**Approach of Data Analysis:** This qualitative analysis examines the linguistic elements in a collection of 20 spam emails gathered from http://www.419scam.org/. While the emails differ in type, they all aim to deceive and manipulate recipients. The analysis is guided by Halliday's Systemic Functional Linguistics (SFL) theory, which allows for an investigation into how particular lexical, grammatical, and orthographic decisions support the spammers' communication objectives.

**Examining Linguistic Characteristics:** The first research question explores the types of linguistic features used by spammers. The analysis shows that lexical choices are often designed to elicit emotional reactions from recipients. For instance, charity-related spam emails include words like "dying woman," "cancer," "humanity," and religious references such as "Lord" and "merciful" to provoke feelings of sympathy, compassion, and trust. Additionally, spammers use time-sensitive expressions (e.g., "pls confirm," "cannot take any telephone calls") to instill urgency and pressure recipients into acting quickly. From a grammatical perspective, spammers commonly use first-person and second-person pronouns ("I," "you," "my," "your") to create a sense of personal connection and direct interaction. The present and future tenses are predominantly employed to engage the reader and promise rewards, while the past tense is mainly used to tell background stories that evoke empathy. Orthographically, spam emails frequently contain errors such as using lowercase "i" instead of "I," spelling mistakes, inconsistent punctuation, and informal abbreviations like "pls." These orthographic inconsistencies unintentionally highlight the informal and deceptive nature of the messages.

**Illustrations from Charity-Related Spam Emails**

**Several examples demonstrate these linguistic patterns:**

- Appendix A features a spam email from "Mrs. Jane Pius," who claims to be donating her belongings as she is on her deathbed. The message uses emotionally charged language related to illness and death, along with religious terms, to boost its credibility.

- Appendix B includes a fundraising email for Haiti earthquake victims, employing words like “earthquake,” “poverty,” and “God” to evoke emotions, while also creating urgency with phrases such as “Immediate response will be appreciated.”
- Appendix C contains an email from an Indonesian village impacted by a tsunami, using terms like “disaster,” “homeless,” and “survive” to elicit sympathy, and employing future tense along with first- and second-person pronouns to build a connection.
- Appendices D and E show similar charity appeals emphasizing urgency and victimhood with words like “death,” “emergency,” “survivors,” and commands urging prompt action.

Across these examples, the lexico-grammatical analysis reveals purposeful word and grammar choices aimed at maximizing emotional influence and encouraging responses. At the orthographic level, frequent errors in spelling, punctuation, and capitalization continue to appear.

**Inactive Account Scam Emails:** Another frequent type of spam revolves around claims of “dormant accounts” holding large sums of money. For example, Appendix F illustrates how spammers use convincing words such as “guarantee,” “necessary information,” and legal-sounding phrases to build trust with recipients. They create a sense of urgency by urging quick responses, sometimes emphasizing this with capitalized commands like “CALL ME.” Orthographic mistakes like “unsuccessfull” and “confisicated,” along with poor punctuation, diminish the emails’ professional appearance. However, this informal tone can sometimes reduce suspicion among certain victims. Grammatically, these emails often describe a fabricated past event—such as the sudden death of a client—using past tense, before shifting to future tense to promise potential rewards.

# DISCUSSION

The analysis shows that Halliday’s tristratal model—especially its focus on lexico-grammar and orthography—serves as a valuable framework for dissecting spam emails. Every choice in vocabulary, grammar, and orthographic form is intentional, crafted to create meanings that manipulate the reader. The findings confirm that spam messages rely on emotional and persuasive language to trick victims, employing strategies like urgency, religious references, personal pronouns, and promises of future rewards. Although orthographic errors indicate informality or lack of professionalism, they also contribute to the distinct linguistic profile of spam. This study enhances our broader understanding of communication tactics used in cybercrime by revealing the linguistic mechanisms behind spam and deception. It aligns with existing research, reinforcing the idea that linguistic analysis—particularly through SFL—can uncover the subtle ways language is manipulated in online fraud. Examining different spam types, including dormant account, lottery, charity, and job vacancy scams, demonstrates how Halliday’s tristratal model offers a robust approach to understanding the linguistic strategies used in these deceptive messages. At the lexical level, spammers carefully choose words that evoke urgency, credibility, or emotional responses—for example, terms related to death and inheritance in dormant account scams, words associated with luck and celebration in lottery emails, or formal vocabulary in job vacancy scams. These deliberate choices aim to shape the reader’s perception and prompt a reaction. Grammatical features help establish a direct connection between the spammer and recipient, primarily through the use of second-person pronouns (“you,” “your”), which personalize the message and boost its persuasive effect. Verb tenses are strategically varied: past tense to tell stories, present tense to state facts, and future tense to promise benefits or consequences. Imperative sentences often appear to subtly pressure recipients into acting immediately. Orthographic elements include intentional capitalization to highlight key terms and grab attention (e.g., “CONGRATULATIONS,” “FINAL NOTICE”), alongside unintentional mistakes like spelling errors, punctuation problems, and inconsistent formatting. While these errors reflect the spammers’ lack of professionalism, they can also help recipients recognize the fraud. Overall, the combined analysis of these linguistic layers reveals how spammers skillfully use language as a tool to build deceptive and persuasive messages that manipulate recipients’ emotions, trust, and sense of urgency. This study underscores the effectiveness of Halliday’s SFL theory and its tristratal model in uncovering the complex linguistic tactics behind spam emails, illustrating how lexical, grammatical, and orthographic features work in tandem to fulfill the communicative aims of cybercriminals.

**Roles of Linguistic Features in Facilitating Deception in Spam Emails:** This section examines how linguistic features operate as instruments of deception and manipulation in spam emails, using Halliday’s Systemic Functional Linguistics (SFL) theory as a framework. The analysis centers on the three metafunctions of language—ideational, interpersonal, and textual—with particular emphasis on the textual function, which exposes how meaning is shaped in spam messages to mislead recipients. Lexical choices in spam emails are intentional and carefully crafted to influence readers’ emotions and perceptions. Spammers deliberately pick words that inspire trust, urgency, or hope, steering recipients toward unwittingly complying with fraudulent requests. Grammatically, the use of imperatives, present and future tenses, and frequent second-person pronouns establishes a direct and compelling interaction, creating a sense of immediacy and personal connection that manipulates the target’s reactions. Orthographic features, such as deliberate capitalization, highlight key points to strengthen the deceptive effect of the messages. Although some spelling and punctuation mistakes reflect the spammer’s lack of professionalism, certain intentional typographical choices aim to draw the recipient’s focus and reinforce important manipulative content. Overall, these linguistic features go beyond typical communication functions by exerting subtle pressure on readers, encouraging swift compliance. The textual metafunction is especially significant, as it organizes the message to covertly guide and influence the recipient’s behavior. This discussion aligns with Halliday’s SFL tristratal model, showing how choices at the lexico-grammatical and orthographic levels are purposefully selected to deceive. It supports (31) view that linguistic choices are intentional and context-dependent, chosen from various options to fulfill specific communicative aims. In summary, this study demonstrates that language in spam emails is carefully designed to deceive and manipulate through strategic use of linguistic features. Halliday’s SFL theory provides an effective lens to uncover how language functions as a powerful tool of manipulation within the realm of cybercrime communication.

# CONCLUSION

# RECOMMENDATIONS

As technology and online communication continue to grow, cybercrimes like spamming have become more widespread and harmful. Spammers use language as a powerful means of deception and manipulation, employing carefully chosen linguistic tactics to deceive and exploit internet users. This study reveals that the lexical, grammatical, and orthographic elements in spam emails are deliberately designed to shape readers' perceptions and behaviors, often by creating a sense of urgency or appealing to emotions to prompt immediate action. Using Halliday's Systemic Functional Linguistics (SFL) theory, especially its tristratal model, the research demonstrates how linguistic features operate on multiple levels to achieve deceptive goals. Language in this context not only communicates information but also manipulates recipients, functioning as a subtle weapon in cybercrime. The intentional use of specific words and language structures reflects spammers' objectives to control and mislead their targets, supporting previous studies on online deception. The findings highlight the need to raise awareness among internet users about the linguistic strategies employed in spam emails. It is important for users to be cautious, verify the authenticity of messages, safeguard personal data, and report suspicious communications. Additionally, sharing experiences and organizing community awareness campaigns can help strengthen collective defenses against cybercrime. For future research, the study suggests broadening the focus beyond lexical, grammatical, and orthographic features to include other linguistic aspects and different forms of cybercrime such as phishing and scamming. Exploring a wider range of spam types will also contribute to a deeper understanding of the language used in electronic deception. In summary, this research offers valuable insights into how language functions as a tool of manipulation in cybercrime, laying groundwork for further studies on how linguistic strategies enable online fraud and victimization.

# REFERENCES

Akopova, A.S. (2013). LINGUISTIC MANIPULATION: DEFINITION AND TYPES. *International Journal of Cognitive Research in Science, Engineering and Education, 1*, 78-82.

Cukier, w., Ngwenyama, O., & Nesselroth-Woyzbun, E. (2008). Genres of spam: Expectations and deceptions. *Scandinavian Journal of Information Systems, 20*(1), 69-92.

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*(1), 74-118. https://doi.org/10.1037/0033-2909.129.1.74

Anafo, C. (2017). *The language of deception: Transitivity analysis of scam email messages* (Master's thesis, University of Education, Winneba). http://ir.uew.edu.gh:8080/handle/123456789/1547

Almoqbil, A., O'Connor, B., Anderson, R., Shittu, J., & McLeod, P. (2021). Modeling deception: A case study of email phishing. *Proceedings from the Document Academy, 8*(2), 1-10. https://doi.org/10.35492/docam/8/2/8

Belli, S., & Bernal, M. (2018). Discursive-linguistic devices and strategies in spam e-mail narratives. *International Journal of Information Communication Technologies and Human Development, 10*(3), 1-13. 10.4018/IJICTHD.2018070101

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

Zuckoff, M. (2005). Annals of crime: The perfect mark. *The New Yorker, 82*(13), 36-42.

Claburn, T. (2005, February 3). *The cost of spam in terms of lost productivity has reached $21.58 billion annually.* InformationWeek. http://www.informationweek.com/story/showArticle.jhtml?articleID=59300834.

Juneja, P., & Pateriya, R. (2014). A Survey on email spam types and spam filtering techniques. *International Journal of Engineering Research & Technology (IJERT), 3*(3), 2309-2314.

Ollmann, G. (2007). *The phishing guide: Understanding & preventing phishing attacks*. IBM Corporation, New York, U.S.A. https://nsi.org/ReferenceLibrary/630.pdf

Lorincz, N. (2023, June 8). *All the different types of emails you need to know about.* OptiMonk. https://www.optimonk.com/different-types-of-emails/

Edwards, M., Peersman, C., & Rashid, A. (2017). *Scamming the scammers: Towards automatic detection of persuasion in advance fee frauds* (Paper presentation). Proceedings of the 26th International Conference on World Wide Web Companion, Perth, Australia. 10.1145/3041021.3053889

Belli, S., & Bernal, M. (2015). Gender identity and emotions in email spam. *International Journal on Collective Identity Research*, *129*(2), 1–12.

Rich, T. (2017). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal, 31*(3), 1-18. 10.1057/s41284-017-0095-0

Mohammad, R. (2020). A lifelong spam emails classification model. *Applied Computing and Informatics.*https://doi.org/10.1016/j.aci.2020.01.002

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.

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

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.

Bernal, M., & Belli, S. (2013). *Virtual ethnography and spam: Fraud and fear in deceptive narratives on the internet (*Paper presentation). Actas del 2º Congreso Nacional sobre Metodología de la Investigación en Comunicación, Segovia. http://uvadoc.uva.es/handle/10324/3035

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

Shafqat, W., Lee, S., Malik, S., & Kim, H. C. (2016). *The language of deceivers: Linguistic features of crowdfunding scams* (Paper presentation). Proceedings of the 25th International Conference Companion on World Wide Web, Canada. http://dx.doi.org/ 10.1145/ 2872518.2889356.

Hiß, F. (2015). Fraud and fairy tales: Storytelling and linguistic indexicals in scam e-mails. *International Journal of Literary Linguistics, 4*(1), 1-23.

Harré, R. (2009). Saving critical realism. *Journal for the Theory of Social Behaviour, 39*(2), 129–143. doi:10.1111/j.1468-5914.2009.00403.x

Jáñez-Martino, F., Alaiz-Rodríguez, R., González-Castro, V., Fidalgo E., & Alegre, E. (2022). A review of spam email detection: Analysis of spammer strategies and the dataset shift problem. *Artificial Intelligence Review, 56*, 1145–1173.

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

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

Dhah, E. H., Naser, M. A., & Ali, S. A. (2019) S*pam email image classification based on text and image features* (Paper presentation). First International Conference of Computer and Applied Sciences (CAS), 148–153. https://Doi.org/10.1109/CAS47 993. 2019. 9075725

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

Eggins, S. (2004). *An Introduction to systemic functional linguistics* (2nd ed.). London: Bloomsbury Academic.

Anafo, C., & Ngula, R. (2020): On the grammar of scam: Transitivity, manipulation and deception in scam emails. *WORD, 66*(1), 16-39. DOI: 10.1080/00437956.2019.1708557

Abosede, A. J., & Onanuga, A. T. (2016). Research design: A Review of features and emerging developments. *European Journal of Business and Management, 8*(11), 113-118.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Obeyd, S. (2021). Research methods in linguistics: An Overview. *Studies in Linguistics, Culture, and FLT, 9*(1), 54-82. 10.46687/SILC.2021.v09i01.004

## APPENDICES

Appendix A

**janepius@stargatesg1.com**

Date: Fri, 15 Jan 2010 07:33:19 +0000 (GMT)
From: “ongoog1@yahoo.com”
Subject: pls confirm

**Dear Beloved**

My Name is Mrs. Jane Pius I am a dying woman who has decided to donate what I have to charity through you. You may be wondering why I chose you. But someone has to be chosen. I am 73years old and was diagnosed for cancer about 2 years ago,immediately after the death of my husband who had left me everything he worked for.I have been touched by the lord to donate from what I have inherited from my late husband to charity through you for the good work of humanity, rather than allow my relatives to use my husband’s hard earned funds inappropriately. I have asked the lord to forgive me all my sins and I believe he has, because He is merciful. I will be going in for an operation, and I pray that I survive the operation. I have decided to WILL/Donate the sum of $5,900,000.00 Million to charity and the victims of the haiti earthquake through you for the good work of the lord, and to help the motherless, less privileged and also for the assistance of the widows. At the moment I cannot take any telephone calls, due to the fact that my relatives are around me and I have been restricted by my doctor from taking telephone calls because I deserve all the rest I can get. I wish you all the best and may the good Lord bless you abundantly, and please use the funds well and always extend the good work to others.If you are interested in carrying out this task,i will inform my Family Lawyer so that he can arrange the release of the funds to you. I know i have never met you but my mind tells me to do this,and I hope you act sincerely.I will pay you 30% of this money if you will assist me because I am now too weak and frigile to do things myself because of my ca ncer.

NB: I will appreciate your utmost confidentiality in this matter until the task is accomplished,as I don’t want anything that will Jeopardize my last wish. please i will appreciate you to kindly get back to me through this email address janepius@stargatesg1.com for further and effective proceedings.

Remain Blessed in The Lord
Mrs. Jane Pius

**Appendix B**

**marycool77@yahoo.com**
http://www.ifc.org/carees

**Dear Sir/Madam,**

My name is mary jones.I would be apreciative if you can help us to donate for the haiti earthquake which many lifes have been lost We have just been granted a funding to head and assist the haiti earthquake, poverty and pubilc policy , if you are interested in donating for the haiti earthquake send your donation to the company accountant through western union or money gram, name: polly lorenz,address: 67 grand ave #4 mount clemens,michigan48043,usa.when you donate send me the MTCN to marycool77@yahoo.com so i can forword it to the company accountant,visit our website or CNN if you need more information,as you donate for the haiti earth quake God will bless you and your family and no bad news of death we come near your family.

Your Immediate response will be appreciated.

Yours In Service.

mary jones

**Appendix C**

**TSUNAMI VICTIMS AIDS APPEAL**

**Dear Sir/Madam.**

We are from a small village in the Banda/Aceh Region in Indonesia affected by the recent Tsunami Quakes/floods disaster that swept through South Eastern Asia. We have been rendered homeless and have lost all we have in life. Many foreign tourists also were affected by the quakes. Since we have no other way to survive as of now and have lost most of our relations and children, we have decided to write this letter of APPEAL FOR DONATIONS. We will be very grateful if you can assist us with any amount of money to enable us start a new lease of life. Our little business have been swept off by the floods and we cannot go and steal. All we need is money to rehabilitate and start business again to make a living. We are sending this mail to many people all over the world for assistance as we cant help ourselves. The United Nations and other world bodies/organisations are helping but it is mostly in Clothes, water and medicaments. So we need your assistance Sir/Madam and we pray that God will reward you abundantly for listening to the voice of the less priviledged and people whose life have been devastated by a natural disaster. Any Donation can be sent to us through our nominated bank account below:

BANK: KOREA EXCHANGE BANK, ITAEWON BRANCH,
SEOUL. SOUTH KOREA
SWIFT CODE: KOEXKRSE,
A/C #: 089-JSD-101464-3,
A/C NAME: MOJEKWU VICTOR,
BENEFICIARY: TSUNAMI AIDS APPEAL

Please do not hesitate to reach us with a copy of the transfer slip for any money sent to our designated account for our records and also for reconciliations with the bank. Your assistance will be appreciated. Thanks for your anticipated cooperation. Mr Teh Ho For: Banda/Aceh Victims of Tsunami Indonesia

**Appendix D**

From: "Economics Community Of West African States (ECOWAS)" <ecowasheads@post.com>
To: <ecowasheads@post.com>
Sent: Monday, 03 January, 2005 20:35
Subject: Tsunami Disaster Aid Raises.
Branch Headquarters: (Rue 27 VoxDar Porte 111 Bamako Mali
Contacts: 00223 6711675 Fax : 00223 228 5553
E-mail: ecowasheads@post.com
Website: www.ecowasbranch70.tripod.com
Ref: 0073220 Date:- 03, Jan 2005
U.N.: Tsunami aid rises to $2 billion

**Attention Sir,**

The ECONOMIC COMMUNITY OF WEST AFRICAN STATES (ECOWAS) wants to draw your attention to the terrible disaster that claims about 140 thousands lives and properties in Thialand, Siri lanka and Indonesia, Pledges of international financial support for countries devastated by this disastser needs emergency financial support, according to the U.N.'s emergency relief coordinator. The estimated death toll in the disaster now is more than 140,000, Ecowas needs your financial aid to sustain the victims affected by this disaster. Also Ecowas has raised an open donation to any body who feels concern to make a generous nonation to aid the victims. Ecowas expects to raised about $1.5 Billion USD. So far, Ecowas has organized to pump 850 40 Ft containers of food items to the countries affected. Some of those supplies began reaching victims in remote areas of Indonesia on Saturday, while relief workers were expected to arrive in Colombo in Sri Lanka, later in the day. No amount of donation like funds, food, medicines, clothes is small, please make your donation today for the survival of the victims and God pay back to those who donate. The money will allow relief workers to feed, clothe, and provide emergency medical services to the affected victims. Payment instruction to the Ecowas Relief Management Coordinator BEN IDOWU

ECO BANK BAMAKO BRANCH MALI WEST AFRICA
BP E 1272 BAMAKO MALI.
Account No:- 440030102018
Swift Code:- ECOCMLBA
Beneficiary:- BEN IDOWU
Correspondent in USA
Citibank New York
Finance Institutions Africa
111 Wall Street
19th Floor / Zone 1
New York 10043
Account:- 36219282
Swift:- CITIUS 33
GOD Bless you as you donate.
Thanks.
Dr. Musa Owo
(Ecowas Procurement Manager)

**Appendix E**

From: "dyspraxia" <dyspraxiafoundation@yahoo.com>
Sent: Tuesday, 04 January, 2005 19:49
Subject: I NEED YOUR ASSISTANCE

THE DYPRAXIA FOUNDATION
8 WEST ALLEY
HITCHIN
HERTFORDSHIRE SGS 1EG
UNITED KINGDOM

The dyspraxia foundation is a charitable foundation headquartered in uk (london) which serves to promote music, theater, art, literature, projects in the social and political arena with a focus on health, as well as science, research, and higher education. Most recently the foundation set up as a foundation that caters for the needs of the poor and the lees privelage in the society The TSUNAMI DISASTER as it is now known the world over took everybody by surprise. It rought with it horror, death and destruction of a very high magnitude that has not been withnessed for a long time.

We are co-orditaing activities towards providing relief materials, shelter and food to the displaced survivors of the disaster. As you are aware over one hundred and fifty thousand innocent people including six thousand tourist perished in the disaster. We are using this medium to solicite and appeal to well meaning organization and individuals to come to their rescue by contributing their own quota towards helping the survivors. To this end we request that you make a

generous donation of at least 100 pound(215 dollars) towards this cause. For further information on how you can be of help please respond to; MR WILLIAM BECKS THE DYSPRAXIA FOUNDATION, LONDON ;UK EMAIL ADDRESS: williamsbecks@london.com TELEPHONE NUMBER :44 - 704 - 010 – 4605
You will be greatly rewarded as you give to the less fortunate in our society. Certificate of appreciation and citation would be issued to those who support this noble cause.
Yours faithfully,
Susan Khan.

**Appendix F**

Attn:......

I am Barrister Daniel Tete , a solicitor at law, personal attorney to Mr.J.C. de Krijger , a national of your country, who used to work as a contractor in Lome Togo. Here in after shall be referred to as my client. On the 30th of April 2000, my client, and their only daughter were involved in a fatal accident along Kpalime express Road. All occupants of the incident unfortunately lost there lives. Since then I have made several enquiries here to locate any of my clients extended relatives, this has also proved unsuccessful. After these several unsuccessful attempts,I decided to searcht-hrough with his name which motivated me to contact you, to locate any member of his family hence I contacted you.

I **have** contacted you to assist in repartrating the fund valued at US$20.5 million left behind by my client before it gets confisicated or declared unserviceable by the Security Finance (bank) where this huge amount were deposited. The said Security Finance Bank has issued me a notice to provide the next of kin or have his account confisicated within the next twenty one official working days. Since I have been unsuccesfull in locating the relatives for over 2years now, I seek the consent to present you as the next of kin to the deceased since you have the same last name, so that the proceeds of this account can be paid to you. Therefore, on receipt of your positive response, we shall then discuss the sharing ratio and modalities for transfer. I have all necessary information and legal documents needed to back you up for this claim. All I require from you is your honest co-operation to enable us see this transaction through. I guarantee that this will be executed under legitimate arrangement that will protect you from any breach of the law. CALL ME FOR MORE DETAILS ON 00228 9071275. Best regards. Daniel Tete (esq)

*******