JEdu Journal of English Education
Volume 5 Number 2, July 2025
e-ISSN 2798-6543
p-ISSN 2798-5164
Pages: 65-74

LINGUISTIC FEATURES OF ONLINE SCAM MESSAGES: A FORENSIC ANALYSIS OF DECEPTIVE COMMUNICATION LANGUAGE

Deliana Wahyu Pradesi[1], Noni Marlianingsih[2]

[1] Universitas Terbuka, Jakarta, Indonesia
[2] Universitas Indraprasta PGRI, Jakarta, Indonesia

Corresponding Author(S): adeliamishbah@gmail.com[1], marlianingsihnoni06@gmail.com[2]

Abstract:
This research investigates the linguistic features commonly used in online scam messages from a forensic linguistic perspective. The researcher uses a qualitative descriptive approach to analyze twenty scam messages collected from SMS, WhatsApp, and email platforms. The data reveal recurring patterns of deceptive language, including impersonation of official institutions, expressions of urgency, persuasive tone, and call-to-action strategies. These linguistic features are used intentionally by scammers to manipulate victims and create a false sense of trust or fear. The findings highlight how language functions as a tool of deception in digital fraud, offering valuable insights for digital literacy education and forensic investigation. This research contributes to understanding deceptive communication and the practical application of forensic linguistics in combating online scams.

Keywords:
Forensic Linguistics; Online Scam; Deceptive Communication

INTRODUCTION

In today's digital era, electronic communication has become an integral part of everyday life. Alongside its benefits, this convenience has also opened new avenues for cybercrime, particularly in the form of online scams. Nowadays, online scams are increasingly common on platforms such as SMS, WhatsApp, and social media. Scammers exploit language as their primary tool to deceive and manipulate individuals into revealing personal information, transferring money, or clicking malicious links. These scam messages often appear legitimate, using persuasive and deceptive linguistic strategies that make them difficult to detect.

Forensic linguistics offers a unique perspective in analyzing such deceptive messages. By examining linguistic structures, vocabulary choices, and discourse patterns, the researcher can identify how language is manipulated to achieve fraudulent intent. This study applies forensic linguistic analysis to identify key linguistic features in scam messages and to understand how language is used as a mechanism of deception.

The purpose of this study is two folds: 1. to describe a linguistic patterns especially written text in online scam messages, and 2. to explore how these features are employed to manipulate recipients. This research is expected to contribute to forensic linguistic scholarship and support broader digital fraud prevention efforts by enhancing public awareness of linguistic cues commonly found in scam communication.

The following research questions guide the analysis: 1. what is the form of written language in linguistic features commonly used to carry out online scam messages? 2. How are these features used to construct deception and manipulate the recipient?

The findings of this study are anticipated to contribute to both academic discourse in forensic linguistics and practical efforts in digital fraud prevention.

1. Forensic Linguistics and Deceptive Communication
   Forensic linguistics is the application of linguistic knowledge to legal and criminal investigations (Coulthard & Johnson, 2007). It examines how language can serve as evidence in various legal contexts, including written threats, confessions, and fraudulent messages. One significant branch of forensic linguistics is the analysis of deceptive communication—messages constructed to mislead or manipulate recipients for unlawful purposes (Olsson, 2008)

2. Scam Discourse Structure
   Scam messages are often formulaic, meaning they follow predictable structures. Chiluwa and Ajiboye (2017) studied email scams and identified five recurring elements: false identity, authority claim, narrative buildup, emotional appeal, and a direct request. These structures create a false sense of legitimacy while manipulating the reader's emotions.

Toma and Hancock (2012) also found that online scammers use language to mimic sincerity, leveraging flattery, urgency, and perceived authority to gain victims' trust.

1. Speech Acts and Manipulation
   Speech act theory (Searle, 1979) helps classify the intent behind scam messages. Many fraudulent messages are directives (e.g., asking for an OTP code), commissives (promising rewards), or assertives (stating false claims). These acts are framed to sound beneficial or urgent, triggering fast, uncritical responses. Grant and MacLeod (2016) emphasize that analyzing these speech acts can help identify deceptive intent even when lexical content seems harmless.

2. Digital Contexts and Cultural Adaptation
   With the rise of digital fraud, scam language has evolved to fit localized contexts (Nurhayati & Nugroho, 2021). For example, Indonesian scams often use institutional references like BPJS, PLN, or BRI, whereas English ones may refer to global entities like Amazon, PayPal, or DHL. This cultural adaptation increases scam plausibility. Moreover, digital scams use platform-specific conventions — such as emoji, short message styles, or WhatsApp formatting — to appear authentic.

   Linguistic Characteristics of Scam Messages

Previous studies have identified several key linguistic traits in scam texts. Common features include:

a. Impersonation of authority (e.g., using names of banks or institutions)
b. Lexical urgency (e.g., "immediately", "urgent", "24 hours only"),
c. Politeness strategies (to appear trustworthy or formal),
d. Call-to-action phrases (e.g., "click the link", "send your data").

These traits are designed to bypass critical thinking and push victims toward quick decisions. Scam messages often follow a predictable discourse pattern: greeting → false claim → time pressure → CTA (Call to Action)

3. Pragmatics and Illocutionary Force

According to speech act theory (Austin, 1962; Searle, 1969), language performs actions, not just conveys information. In scam messages, commands ("Klik link ini sekarang") in English ("Click this link now") and threats ("Akun Anda akan diblokir") in English ("Your account will be blocked") (carry illocutionary force — they attempt to make the recipient do something. Deceptive messages rely on directive speech acts, often masked with politeness strategies (Brown & Levinson, 1987) to reduce resistance. Politeness functions as a tool for manipulation — what sounds kind may hide harmful intent.

4. Relevant Previous Research

Coulthard and Johnson (2007) emphasize that in order to construct a sense of legitimacy and authority, scammers frequently rely on formulaic language and the manipulation of pragmatic features. These include commonly used expressions, structured openings and closings, and politeness strategies that mimic institutional or corporate communication Such language use is not accidental; it is deliberately designed to reduce suspicion and increase compliance from recipients. Olsson (2004) further draws attention to the increasing use of modal verbs (such as may, must, can, should) and ambiguous referents (e.g., your account, this message, the prize) in scam messages. These linguistic features contribute to a tone of urgency and authority, while simultaneously avoiding precise detail that could reveal the scam's lack of authenticity.

In addition, more recent studies on digital fraud have identified how scam language is increasingly adapted to suit the socio-cultural context of the target audience, the platform used for delivery, and even the intended demographic. For example, research has shown that scams distributed via SMS are often more concise and use abbreviated language, while WhatsApp or email-based scams may include visual elements like logos or hyperlinks to mimic official correspondence. Cultural adaptation is also critical—messages targeting Indonesian users may employ religious references, honorifics, or local institutions to foster trust, while English-language scams might focus more on legal-sounding jargon or international authority figures to achieve a similar effect.

Building on these foundational frameworks, the present study investigates how these linguistic strategies are implemented and operationalized in scam messages disseminated via commonly used digital messaging platforms. By analyzing texts in both Indonesian and English, this research aims to identify shared patterns as well as

culturally specific markers of deception. The study also seeks to explore how scammers exploit platform-specific affordances (such as message formatting, tone, and interactivity) to maximize the persuasive impact of their fraudulent communication. This research builds upon these frameworks to explore how such features are realized in Indonesian and English-language scam messages found on common messaging platforms.

5. Forensic Linguistics in Digital Crime Contexts
   As cybercrime continues to rise rapidly in the digital age, the need for forensic linguistic tools and methods to analyze and profile language used in online criminal activities has become increasingly critical. One of the key contributions to this field is the development of linguistic fingerprinting, a method that identifies consistent patterns in a speaker or writer's language use.

   Grant (2013) emphasized that individuals often leave behind unique linguistic traces—such as word choice, syntactic structure, and stylistic preferences—which can be used to attribute authorship in anonymous or deceptive messages. Similarly, Tim Grant and Alison (2011) demonstrated how linguistic evidence can be applied to distinguish between genuine and fraudulent communication, particularly in the context of threats, fraud, and impersonation.

   In online scam cases, such linguistic profiling can serve as a crucial tool for uncovering the identity or behavioral patterns of perpetrators, especially when conventional investigative methods are limited. These linguistic cues can also be used to develop early warning systems, identify scam typologies, and support legal proceedings by presenting evidence rooted in language analysis. As digital platforms become the primary medium for criminal manipulation—through emails, SMS, social media, and instant messaging—linguistic forensics plays an increasingly vital role in digital investigations and cybersecurity. Therefore, integrating forensic linguistics into digital crime prevention frameworks offers promising potential in both academic research and law enforcement practice.

METHOD

This study applies (Creswell, 2017) criteria of credibility, dependability, and confirmability in validating qualitative data, this method for ensuring the trustworthiness of this research:

a. Credibility
   Credibility refers to the accuracy and truthfulness of the research findings in representing the data. To enhance credibility: Prolonged engagement and familiarity with data: The researcher carefully examined each message multiple times to deeply understand the linguistic nuances and manipulation strategies. Triangulation of sources: Messages were collected from multiple platforms (SMS, WhatsApp, and email), providing diverse contexts and forms of scam discourse. Peer debriefing: Portions of the categorized data and analysis were reviewed by academic peers in linguistics to ensure interpretations were reasonable and not overly biased. Member checking (adapted): While the senders of scam messages could not be contacted for ethical and practical reasons, informal validation was conducted by comparing patterns with reports and descriptions of scams from credible cybersecurity sources.

b. Dependability
Dependability concerns the stability and consistency of the research process. This was addressed by: Audit trail documentation: The researcher kept systematic records of message collection, coding categories, and analytical notes to allow future replication or review of the analysis process. Transparent coding framework: Clear criteria were used to define lexical, syntactic, pragmatic, and discourse features, ensuring that analysis followed consistent procedures. Use of analytical memos during the coding process also contributed to maintaining methodological consistency throughout the study.

c. Confirmability
Confirmability ensures that the findings are shaped by the data and not by researcher bias. This was achieved through: Reflexive journaling: The researcher maintained a reflective log to record decisions, assumptions, and potential biases during the interpretation process. Cross-checking with external literature: Findings were compared with existing studies and theoretical frameworks on linguistic deception to ensure alignment with recognized linguistic patterns. Data transparency: Selected anonymized message excerpts were included in the analysis section to illustrate how conclusions were drawn directly from the data.

RESULTS AND DISCUSSION

Results

The analysis of 20 scam messages revealed several consistent linguistic patterns. Most messages followed a similar structure: greeting, false claim (such as winning a prize or having a banking issue), expression of urgency or threat, and a call-to-action (CTA). Deceptive language was consistently used to manipulate the recipient's emotions and judgment.

Table 1 Summary of Linguistic Strategies in Scam Messages

No	Strategy	Linguistic Features	Function	Example
1	**Impersonation of Institutions**	Use of formal greetings, institutional names/logos, official-sounding terms	Creates false authority and credibility	"Selamat! Anda terpilih sebagai pemenang dari Bank Indonesia."
2	**Visual-Linguistic Formatting**	Use of logos, headers, formal structure, pseudo-official layout	Simulates real institutional messages to reduce suspicion	Fake BRI letter with autodebit notice and corporate branding
3	**Semantic Manipulation**	Phrases implying passive consent (e.g., "Jika tidak konfirmasi dianggap setuju")	Traps user by misrepresenting agreement mechanisms	"Jika tidak konfirmasi, maka akan dianggap SETUJU."
4	**Urgency and Threat**	Use of time pressure, warnings (e.g., "akun Anda akan dibekukan")	Triggers emotional response and discourages critical thinking	"Harap segera konfirmasi dalam 1x24 jam sebelum akun Anda dibekukan."
5	**Politeness and Manipulative Tone**	Use of honorifics, courteous expressions (e.g., "mohon	Builds trust and compliance using social norms of politeness	"Mohon bantuannya untuk mengisi data agar proses cepat

No	Strategy	Linguistic Features	Function	Example
		bantuannya", "Bapak/Ibu")		selesai."
6	**Ambiguity and Vagueness**	Lack of specific details, vague timeframes or instructions	Prevents verification and encourages quick compliance	"Mulai nanti malam... semua data di isi semua dengan benar."
7	**Direct Call-to-Action (CTA)**	Imperative sentences, hyperlinks, request to fill forms or submit OTP	Leads users to phishing sites or extracts sensitive information	"Klik link berikut dan isi formulir pengiriman hadiah Anda."
8	**Psychological Framing**	Framing scams as security procedures, system errors, or service upgrades	Shifts perceived motive to safety or improvement, reducing resistance	"Sistem kami mendeteksi aktivitas tidak biasa… kirimkan kode 6 digit."

Discussion

1. Linguistic Strategies in Scam Messages
   a. Impersonation of Institutions
   Example: "Selamat! Anda terpilih sebagai pemenang dari Bank Indonesia." Translation: "Congratulations! You have been selected as the winner from Bank Indonesia." Scammers frequently claim to represent trusted institutions such as banks, delivery services, or government bodies. This tactic creates false credibility and lowers the victim's suspicion.

   Example: Fraudulent "BRI Monthly Fee" Announcement Letter (Image-Based Scam).

   Translation:
   ANNOUNCEMENT

   Dear Sir/Madam,
   Valued Customer,

   In connection with the updates to Bank BRI's services, to improve quality and customer
   convenience when transacting via BRI mobile/internet banking:

Starting tonight at midnight (the change of day and date), all transaction fees will be converted to a monthly fee. The current transaction fee of Rp6,500 per transaction will be replaced with a new fee of:

Rp150,000 per month (Auto-debited from the savings account), with unlimited transactions.

To trial this new tariff scheme over the next 6 months, BRI is requesting your AGREEMENT or Confirmation, with the following options:

b. *Do you agree to the new monthly tariff of Rp. 150,000, or If you do not agree, and prefer the old tariff of Rp6,500 per transaction (because you rarely transact), then please confirm using the form sent to you. Make sure all data is filled in correctly.*
Note: If you do not confirm, it will be considered as AGREEMENT. A charge of Rp150,000 will be debited monthly from your BRI savings account. The amount will be deducted regardless of whether there are transactions.

THANK YOU
e-Pay BRI BRILink Call BRI 14017 / 1500017 | www.bri.co.id

The scam message, designed as an official-looking announcement from Bank BRI, claims that starting from the next billing cycle, customers will be charged a monthly flat fee of Rp150.000 instead of the previous transaction-based fee of Rp6.500 per transaction. It pressures recipients to confirm or otherwise be considered as agreeing to the new fee. The message is formatted to resemble a formal letter, complete with BRI logos, service links (e.g., e-Pay BRI, BRILink), and contact numbers, and it includes phrases like "Autodebit dari rekening tabungan" and "Unlimited transaksi."

Linguistic Features Identified:

Visual Deception & Formatting: The use of BRI logos, formal formatting, and layout mimics a corporate announcement to gain credibility. This is a multimodal deception combining text and branding visuals.
Semantic Manipulation: Terms like "PERSETUJUANNYA", "KONFIRMASI", and "jika tidak ada konfirmasi maka dianggap SETUJU" are used to trap the user with a sense of passive consent— an unethical framing strategy.

Threat of Loss: The line "Adanya transaksi atau tidak tetap akan di potong" applies coercion by
stating that the fee will be deducted regardless, enhancing urgency.

Institutional Impersonation: The contact numbers (14017, etc.) and links to "www.bri.co.id" are meant to imply authenticity, although scammers often use similar-looking fake links outside the visual area.

Ambiguity and Vague Terms: The message avoids giving specific details about user accounts, timelines, or verification mechanisms. It relies on vague language such as "mulai nanti malam" and "semua data di isi semua dengan benar" which weakens its credibility upon close inspection.

Analysis:

This example showcases how scammers utilize visual-linguistic impersonation to simulate institutional authority. The language strategy involves coercive consent (passive agreement through silence), psychological pressure (financial penalty), and ambiguity. These techniques align with strategies noted by Coulthard & Johnson (2007) and Gibbons (2003) in institutional deception cases. The structured layout mimics genuine banking announcements, but linguistic markers—such as grammatical awkwardness ("semua data di isi semua dengan benar") and unprofessional formatting—can signal inauthenticity to trained eyes.

This message also reflects a growing trend in Indonesia where scammers integrate visual branding and localized terms into digital fraud attempts. It is not only the linguistic content but also the visual-semiotic cues that play a critical role in deceiving the audience.

c. Expressions of Urgency and Threat
Example: "Harap segera konfirmasi dalam 1x24 jam sebelum akun Anda dibekukan."

Translation: "Please confirm within 1x24 hours before your account is frozen."

Urgency is a common feature in scam messages, pushing the victim to act quickly. Scammers use deadlines or consequences (e.g., account closure) to create emotional pressure.

d. Politeness and Manipulative Tone

Example 1:
"Mohon bantuannya untuk mengisi data agar proses cepat selesai."

Translate: "Kindly assist by filling in the data so the process can be completed quickly."

Analysis:
Scam messages often use polite language to appear respectful and trustworthy. This strategy manipulates social norms of politeness to mask malicious intent.

Example 2:
Original (Indonesian):
"Silakan kirimkan kode OTP yang Bapak/Ibu terima untuk verifikasi ulang akun demi keamanan."

Translation:
"Please send the OTP code you received for re-verifying your account for security purposes."

Analysis:
This sentence uses formal and polite tone ("Silakan", "Bapak/Ibu", "demi keamanan") to create a sense of legitimacy. It exploits the user's instinct to comply with respectful requests, especially when framed as security procedures. However, legitimate institutions never ask for OTPs via chat — this is a key red flag.

Example 3:
Original (Indonesian):
"Kami mohon pengertiannya, sistem kami mendeteksi aktivitas tidak biasa. Untuk itu, harap kirimkan 6 digit kode yang baru saja dikirim ke nomor Anda."
Translation:
"We ask for your understanding, our system detected unusual activity. Therefore, please send the 6-digit code just sent to your number."

Analysis:

This message builds urgency and implies threat ("aktivitas tidak biasa"), while softening it with polite and formal language ("kami mohon pengertiannya"). The manipulative tone adds psychological pressure, pushing users to respond out of fear and a sense of duty.

Scam messages often use polite language to appear respectful and trustworthy. This strategy manipulates social norms of politeness to mask malicious intent.

e. Direct Call-to-Action (CTA)
Example: "Klik link berikut dan isi formulir pengiriman hadiah Anda."

Translate: "Click the following link and fill out the prize delivery form."

CTAs are used to direct victims to fake websites or request sensitive information. The language is direct and imperative, urging immediate response without scrutiny.

2. Interpretation and Theoretical Connection
The linguistic features identified in the scam messages are consistent with previous research. Olsson (2008) noted the use of urgency and impersonation in deceptive texts, which is evident in the analyzed data. Coulthard & Johnson (2007) discussed the formulaic nature of scam discourse, matching the structural patterns found in this study. This study also reinforces the idea that scammers strategically use pragmatics and discourse organization to construct believable lies.

CONCLUSION

This research explored the linguistic features of online scam messages through the lens of forensic linguistics. The findings revealed that scam messages commonly employ a structured pattern consisting of a greeting, a false claim, urgency or threat expressions, and a direct call-to-action. Key strategies used include impersonation of authority, use of polite and manipulative language, expressions of urgency, and imperative commands.

These linguistic features are designed to exploit psychological pressure, social norms, and digital habits of the victims. The analysis supports previous research on deception and highlights the effectiveness of linguistic manipulation in digital fraud.

Understanding the language of scams is essential not only for academic purposes but also for public awareness and prevention. This study contributes to the growing body of forensic linguistic research and emphasizes the importance of interdisciplinary approaches in tackling cybercrime.

REFERENCE

Chiluwa, I. M., Chiluwa, I., & Ajiboye, E. (2017). *ONLINE DECEPTION: ADISCOURSE STUDY OF EMAIL BUSINESS SCAMS. Deception and deceptive communication: motivations, recognition techniques and behavioral control*. Nova Science Publicher, Inc.

Coulthard, M., & Johnson, A. (2007). *An Introduction to Forensic Linguistics: Language in Evidence*. Routledge.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Gibbons, J. (2003). *Forensic Linguistics: An Introduction to Language in the Justice System*. Blackwell Publishing.

Grant, T. (2012). *TXT 4N6: method, consistency, and distinctiveness in the analysis of SMS text messages*. JL & Pol'y, 21, 467.

Nurhayati, E., & Nugroho, A. (2021). Language features in online fraud: A case study of phishing emails targeting Indonesian users. *Journal of Forensic Linguistics and Cybercrime Studies*, 4(1), 33–47.

Olsson, J. (2008). Forensic Linguistics: Second Edition. Continuum.

Searle, J. R. (1969). *Speech Acts: An Essay in the Philosophy of Language*. Cambridge University Press.

Searle, J. R. (1979). *Expression and Meaning: Studies in the Theory of Speech Acts*. Cambridge University Press.

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.

Vrij, A. (2008). *Detecting Lies and Deceit: Pitfalls and Opportunities*. John Wiley & Sons.