

Speech Acts in Social Media Fraud: Manipulative Communication Strategies on WhatsApp and Facebook

Nur Lailiyah
Universitas Nusantara PGRI Kediri
Lailiya86@unpkediri.ac.id*

Favorita Kurwidaria
Universitas Sebelas Maret
favorita.kurwidaria282@gmail.com

Monika Widyastuti Surtikanti
Unika Santo Agustinus Hippo
m.surtikanti@sanagustin.ac.id

Galuh Kirana Dwi Areni
Universitas Negeri Semarang
galuhunnes@gmail.com

Setyo Prasiyanto Cahyono
Universitas Dian Nuswantoro
setyo.cahyono@dsn.dinus.ac.id

Farida Indri Wijayanti
UIN Raden Mas Said
faridaindri25@gmail.com

Abstract

This research aims to investigate the role of speech acts in fraudulent activities on social media platforms, particularly WhatsApp and Facebook, through a pragmatic framework. The primary goal is to identify the manipulative communication strategies employed by perpetrators to deceive and influence victims. A qualitative-descriptive methodology was adopted, with data collected from conversation screenshots and communication recordings sourced from victims' case reports in WhatsApp and Facebook ($n = 39$). The data were analyzed using the speech act theory by Austin and Searle, along with Grice's concept of implicature. The findings reveal that directive and commissive speech acts are central to the perpetrators' manipulative strategies, often combined with hidden implicatures intended to create a sense of urgency, establish false trust, and foster emotional dependency in victims. These findings contribute to a deeper understanding of the communicative tactics used in social media fraud. Ultimately, this research offers valuable insights into the dynamics of online deception, highlighting the importance of enhancing digital literacy and advancing strategies for cybercrime prevention. This study also provides a foundation for further research on communication patterns in digital fraud.

Keywords: Fraud, Manipulative Communication, Pragmatics, Social Media, Speech Acts

INTRODUCTION

The development of digital technology has greatly facilitated communication and transactions across various social media platforms (Setiadi, 2021). However, behind these advantages, platforms such as WhatsApp and Facebook have also become fertile ground for criminal activities, including fraud. Social media fraud typically involves perpetrators who exploit false identities and manipulative communication strategies to influence their victims. The methods used vary, ranging from the distribution of fake links and promises of large rewards to subtle threats, all intended to gain illegal advantages (Fatimah, 2023). This issue has grown in complexity and frequency alongside the significant rise in digital transactions in Indonesia, which opens up

more opportunities for such criminal acts in the real-time, non-face-to-face digital environment (Bank Indonesia, 2023; Kominfo, 2023).

In response to this growing threat, the importance of digital literacy in preventing fraud is widely acknowledged. The government, through the Ministry of Communication and Informatics, has initiated various educational programs, including services like CekRekening.id, which allows users to verify the authenticity of bank accounts used in online transactions (Wijaya & Sari, 2022). Previous research and reports have often focused on technical modus operandi, such as phishing links, or have emphasized the financial losses resulting from the surge in digital transactions, without deeply investigating the

linguistic elements that facilitate these crimes (Putri & Kurniawati, 2023; Bank Indonesia, 2023).

In the context of linguistics, social media fraud can be analyzed through a pragmatic lens, particularly by examining the speech acts employed by perpetrators to manipulate victims. These manipulative strategies include the use of directive and commissive speech acts, as well as hidden implicatures, all of which are designed to influence the victim's perception and response (Lailiyah, 2021). This study aims to understand the patterns of speech acts in social media fraud cases, thereby contributing to prevention efforts through the development of communication literacy and more responsive policy frameworks.

A linguistic examination of fraud strategies is essential to understand how language is used manipulatively in criminal acts (Rahman, 2023). Language serves as the primary tool used by perpetrators to shape perceptions, instill trust, or create a sense of urgency in victims. Analyzing speech acts, including directives and commissives, can uncover patterns of manipulative communication employed in fraudulent schemes. For instance, speech acts such as false promises or subtle threats are often used to exploit victims' emotional vulnerabilities. From a pragmatic perspective, this study is relevant for understanding implicatures and implied meanings that often serve as key elements in fraudulent messages. Such investigations can also help identify specific linguistic features that signal manipulation, thus contributing to the development of technology-based fraud detection tools, such as chatbots capable of analyzing language in digital communication.

This research holds significant value in supporting digital security efforts. With the rise of digital transactions and the widespread use of social media, the number of fraud cases has also continued to increase. According to a report by Bank Indonesia, the high value of digital transactions in Indonesia underscores the urgency of protecting the public against crimes that exploit such platforms. A deeper understanding of

manipulative communication strategies can help improve digital literacy among the public, particularly in recognizing the modus operandi of fraudsters.

Furthermore, this study can provide valuable input for policy development, such as the creation of linguistics-based early detection systems for social media platforms. This aligns with the efforts of the government and financial institutions to strengthen consumer protection in digital transactions and to restrict the operational space of cybercriminals. Academically, this research enriches the field of pragmatics by applying its principles to contemporary social issues, such as online fraud, thereby contributing not only to linguistics but also to the broader domain of cybersecurity.

Previous research has revealed various aspects of social media fraud, yet it has not specifically explored the linguistic dimension, particularly the manipulative communication strategies employed by perpetrators. A study conducted by Putri & Kurniawati (2023) highlighted technical modus operandi such as the use of phishing links and fake accounts but did not address how language is used to influence victims. Another approach by Kominfo (2023) focused on digital literacy to raise public awareness about fraud risks, without examining the role of language in the manipulation process. Meanwhile, a report by Bank Indonesia (2023) linked fraud to the surge in digital transactions, emphasizing financial losses without investigating the linguistic elements that facilitate the success of such crimes.

While valuable, these approaches are critically limited because they describe the tools of deception (e.g., fake links) and its consequences (e.g., financial loss) without dissecting the core engine of the manipulation: language. By focusing on the "what" and not the "how," prior studies leave a significant analytical gap. Ignoring the role of speech acts means failing to understand the precise linguistic actions perpetrators perform, how they command, promise, and threaten, to psychologically disarm a victim. This oversight is crucial because fraud is not

merely a technical failure but a communicative one. Without a pragmatic analysis of the language used, prevention strategies remain reactive, addressing the symptoms of fraud rather than the root linguistic tactics that ensure its success.

This study aims to fill that gap by analyzing manipulative communication strategies from a pragmatic perspective. It applies speech act theory and the concept of implicature to understand how fraudsters utilize language as a primary tool for manipulation. Through this approach, the research not only enriches academic discourse in the field of linguistics but also offers practical contributions to the development of digital literacy strategies and language-based security solutions to prevent cybercrime. A deeper understanding of these manipulative strategies can provide valuable input for policy development, such as creating linguistics-based early detection systems, thereby strengthening consumer protection and contributing to the broader domain of cybersecurity.

METHODOLOGY

Research Design

This study employs a qualitative approach aimed at exploring in depth the manipulative communication strategies used by fraud perpetrators on social media, particularly on the WhatsApp and Facebook platforms. The qualitative approach was chosen because it allows for the analysis of the social, cultural, and linguistic interaction contexts that underlie speech acts in fraud cases (Creswell, 2013; Miles et al., 2019).

Pragmatic Analysis Method

The method employed in this study is pragmatic analysis, aimed at examining the manipulative speech acts found in fraudulent messages. This approach refers to Speech Act Theory by Searle (1969), which categorizes speech acts into locutionary acts (the utterance itself), illocutionary acts (the intended meaning of the utterance), and perlocutionary acts (the effect of the

utterance on the listener). The main focus of this research is on analyzing directive speech acts (e.g., requests, threats) and commissive speech acts (e.g., promises, offers), which are frequently used by perpetrators to influence their victims (Grice, 1975; Searle, 1969a).

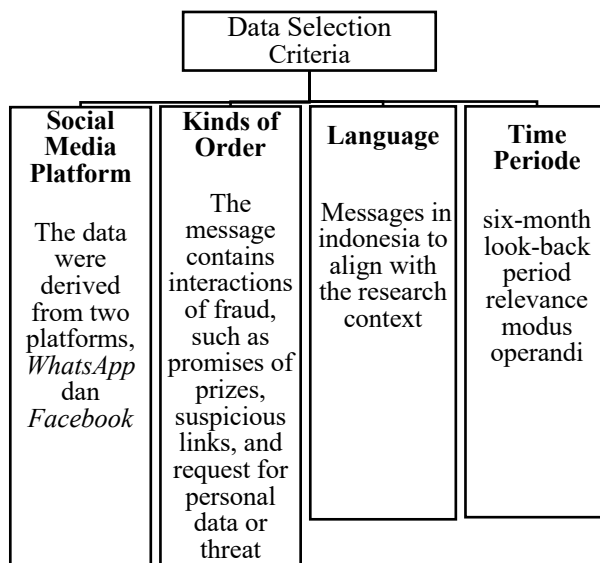
In addition, this study examines conversational implicature, the implied meanings that arise from the context of the utterance. The analysis of implicature is relevant for understanding linguistic manipulation strategies employed by fraudsters, such as creating a false sense of urgency or obscuring information to deceive the victim (Brown & Levinson, 1987).

A total of 39 data were collected using a documentation method, which involved gathering fraudulent messages circulated on WhatsApp ($n = 23$) and Facebook ($n = 16$). The data selection criteria is presented in Figure 1. The data were chosen based on three considerations. First, authenticity is the foundational criterion; the data selected must consist of verified, genuine fraudulent messages to ensure the analysis is grounded in real-world manipulative practices. Second, the completeness of the interaction is vital for a pragmatic study, as it allows for an analysis of the sequential development of speech acts and how perpetrators escalate their strategies over the course of a conversation. Finally, the principle of data richness will guide the selection, prioritizing messages that clearly and explicitly demonstrate the manipulative speech acts, such as directives and commissives, that are the focus of the study.

The researcher employed content analysis techniques to identify recurring communication patterns and manipulation strategies. Data were analyzed systematically to uncover the relationships between the forms of speech acts, their usage contexts, and their communicative impacts on victims (Krippendorff, 2018). This approach is expected to contribute to a deeper understanding of the linguistic aspects of social media fraud and to serve as a foundation for the development of language-based policies or detection tools for cybercrime. The data selection criteria used

in this study are illustrated in the following chart.

Figure 1. Data Selection Criteria



The data analysis process was carried out using a pragmatic approach, focusing on locutionary, illocutionary, and perlocutionary speech acts to understand the intentions and impacts of manipulative messages. The study also explored implicatures, namely, the implied meanings within the messages, and patterns of manipulative strategies such as the creation of urgency or the exploitation of the victim's emotions. The data were analyzed systematically through several stages: message collection, categorization based on types of speech acts, coding of linguistic elements, contextual analysis of the communicative situation, and interpretation of findings grounded in pragmatic theory.

The analytical framework of this study is based on Speech Act Theory employed to examine the forms, functions, and effects of manipulative communication. The primary focus is on violations of conversational maxims, such as quality and quantity, as well as linguistic strategies used to deceive victims. Data validation was conducted through triangulation from multiple sources, expert validation by linguists, and audit trails of the analysis process to ensure reliability. Through this approach, the study contributes to a deeper understanding of linguistic

manipulation strategies in digital fraud and their relevance to digital security in the social media era.

Results and Discussion

Forms of Speech Acts in Social Media Fraud

This study reveals that fraudulent messages on social media can be thoroughly understood and analyzed through the framework of speech acts, which are divided into three primary dimensions: locutionary, illocutionary, and perlocutionary acts. These dimensions are essential for understanding the manipulative strategies employed by perpetrators to exploit their victims' vulnerabilities. Each dimension plays a distinct yet interconnected role in the communication process within fraudulent messages.

The locutionary, illocutionary, and perlocutionary acts are intricately woven together in the tactics used by fraudsters to manipulate their targets. By examining how each of these dimensions functions within fraudulent messages, it becomes clear how social media fraudsters exploit linguistic devices and psychological triggers to influence their victims. This study not only provides insight into the nature of online fraud but also suggests potential strategies for identifying and preventing such deceptive tactics in digital communication. Understanding these speech act dimensions can help raise awareness of the linguistic and psychological mechanisms behind social media fraud, enabling users to better recognize and resist manipulative messages.

Analysis of Locutionary Acts

Locutionary acts refers to the actual utterance or message itself, the words, phrases, and sentences that are spoken or written. In the context of social media fraud, the locutionary act is primarily concerned with the content of the message. Fraudulent messages typically use language that is carefully crafted to appear credible, trustworthy, or urgent. The choice of words in these messages is often deliberate, designed to lower the victim's

defenses and draw them in. This includes the use of persuasive vocabulary, emotive expressions, and seemingly logical claims. The locutionary dimension sets the stage by providing the message that captures the attention of the reader, but it alone does not trigger the full manipulation process. An example of a locutionary act is as follows:

Table 1. Forms of Locutionary Speech Acts

Forms	Utterances
Direct statement	"Selamat Anda memenangkan hadiah Rp.10 juta!" (Congratulation! You have won a prize of IDR 10 million!)
Rhetorical Questions	"Ingin uang cepat tanpa syarat?" (Do you want quick money without any conditions?)

The table highlights how locutionary acts are used in fraudulent messages to capture the victim's attention. Direct statements, like "Selamat Anda memenangkan hadiah Rp.10 juta!" (Congratulations! You have won a prize of IDR 10 million!), make bold claims that entice the victim with false rewards. Rhetorical questions, such as "Ingin uang cepat tanpa syarat?" (Do you want quick money without any conditions?), exploit the victim's desire for easy gain, urging them to act without directly demanding it. Both types of utterances are designed to trigger curiosity and emotions, leading the victim to take action, despite the misleading nature of the message. These locutionary acts set the stage for further manipulation.

The analysis of locutionary acts focuses on the literal meaning of the utterance itself, the words and sentences as they are written. In social media fraud, the locutionary act is not merely a statement but a calculated linguistic construction designed to establish the scam's foundational premise. For instance, the direct statement, "Selamat Anda memenangkan hadiah Rp.10 juta!" (Congratulations! You have won a prize of IDR 10 million!), presents a specific

propositional content: the victim has won money. From a theoretical standpoint, the perpetrator's primary goal at this stage is to craft a proposition that is clear, attention-grabbing, and emotionally appealing. The truth value of this proposition is irrelevant to the fraudster; what matters is that its literal meaning serves as the necessary groundwork for the subsequent manipulative illocutionary force, thereby setting the stage for persuasion and deception.

Analysis of Illocutionary Acts

Illocutionary acts deals with the intention behind the message, what the speaker is trying to achieve through the message. In fraud, the illocutionary act is where the manipulation truly begins. Perpetrators typically aim to persuade the victim to take action, such as sharing personal information, transferring money, or clicking on a harmful link. Illocutionary acts include directives (commands, requests), assertives (statements of fact), and commissives (promises or offers). In fraudulent social media messages, these acts are often disguised under the pretext of friendly advice or an urgent request. For instance, a fraudulent message may assert the need for immediate financial help while simultaneously providing false reassurances or promises of rewards, thereby triggering compliance from the victim. The following are the dominant forms of illocutionary acts.

Table 2. Forms of Illocutionary Speech Acts

Forms	Utterance
Directive	"Kirimkan nomor rekening Anda sekarang!" (Send your account number now!)
Commissive	"Uang Anda akan dikembalikan setelah proses selesai." (Your money will be refunded after the process is completed)
Declarative	"Pesan ini resmi dari bank kami." (This message is officialy from our bank)

The table outlines how illocutionary acts are used to manipulate victims. Directives, like "*Kirimkan nomor rekening Anda sekarang!*" (Send your account number now!), issue clear commands, pressuring the victim to take immediate action. Commissive, such as "*Uang Anda akan dikembalikan setelah proses selesai.*" (Your money will be refunded after the process is completed), offer promises to build trust and convince the victim to comply, creating a false sense of security. Declaratives, like "*Pesan ini resmi dari bank kami.*" (This message is officially from our bank), assert authority to lend legitimacy to the message, further manipulating the victim into believing the scam is genuine. These illocutionary acts work together to persuade the victim to act without skepticism.

The illocutionary act represents the speaker's underlying intention and is the core of the manipulation strategy. Fraudsters predominantly employ directive and commissive speech acts, as defined by Searle (1969), to influence their victims. The utterance, "*Kirimkan nomor rekening Anda sekarang!*" (Send your account number now!), functions as a directive speech act. Its illocutionary force is to command, aiming to compel the victim into immediate compliance without contemplation. This tactic exploits the typical function of directives, which is to get the hearer to perform an action, but in a context of manufactured urgency and authority designed to suppress the victim's critical judgment.

Simultaneously, fraudsters use commissive acts to build a facade of trustworthiness. The promise, "*Uang Anda akan dikembalikan setelah proses selesai*" (Your money will be refunded after the process is completed), is a commissive that commits the perpetrator to a future action. According to speech act theory, a promise is only felicitous if the speaker genuinely intends to carry it out. The manipulation here lies in the deliberate violation of this sincerity condition. The fraudster exploits the victim's expectation of sincerity to create a false sense of security, which in turn makes

the victim more receptive to the primary directive of sending money or personal information. This combination of directive pressure and deceptive commissive assurances is a powerful tool for achieving the intended perlocutionary effect of compliance.

Analysis of Perlocutionary Acts

Perlocutionary acts refer to the effects that the message has on the victim, which represent the primary objective of the fraudster. The following are the perlocutionary effects identified in this study.

Table 3. Forms of Perlocutionary Speech Acts

Forms	Effect of Utterance
Compliance	The victim feels pressured or motivated to follow instructions, such as clicking on a phishing link or providing sensitive information.
Confusion	The use of complex language or ambiguity often causes confusion, making it easier for the victim to be manipulated
fear	Some messages threaten the victim, for example " <i>Akun Anda akan diblokir jika tidak segera diverifikasi.</i> " (Your account will be blocked if not verified immediately) This perlocutionary act shows the perpetrator's success in exploiting the victim's emotional and cognitive aspects to achieve their goal.

The table explains how perlocutionary acts are used to influence the victim's response. Compliance occurs when the victim feels pressured or motivated to act, such as clicking on a phishing link or sharing sensitive information. Confusion arises from the use of complex or ambiguous language, which disorients the victim and makes them more susceptible to manipulation. Fear is

triggered when messages threaten the victim, like "Akun Anda akan diblokir jika tidak segera diverifikasi." (Your account will be blocked if not verified immediately), exploiting emotional and cognitive vulnerabilities to prompt immediate action. These perlocutionary effects manipulate the victim's emotions, leading them to follow through on the scam.

Linguistic Characteristics in Social Media Fraud Messages

The linguistic characteristics employed in fraudulent messages on WhatsApp and Facebook were analyzed based on three main aspects: lexical features, syntactic patterns, and pragmatic elements. Through the analysis of these linguistic features, the study provides a deeper understanding of how fraudulent messages on WhatsApp and Facebook are constructed to exploit cognitive biases and emotional vulnerabilities, ultimately leading to successful manipulation and deception.

Lexical Features

In terms of lexical features, the language used in fraudulent messages often includes specific word choices designed to create urgency, trust, or emotional manipulation. Fraudsters tend to use persuasive vocabulary that makes the message appear credible, while simultaneously prompting an emotional response from the victim. This could include terms that suggest authority, desperation, or exclusivity, all of which are meant to lower the victim's defenses and encourage compliance.

Table 4. Lexical Features

Lexical Features	Utterance
Persuasive Vocabulary	"Selamat! Anda terpilih sebagai pemenang undian Rp10 juta." (Congratulations! You have been selected as the winner of the IDR 10 million lottery.)

Technical or Formal Terms	"Harap segera lakukan verifikasi akun Anda melalui tautan berikut." (Please immediately verify your account through the following link.)
---------------------------	---

The use of lexical features in persuasive vocabulary predominantly includes words such as "selamat" (congratulations), "hadiah" (prize), "resmi" (official), and "gratis" (free) to generate enthusiasm or a sense of certainty. Utterances like "selamat" (congratulations) and "pemenang" (winner) evoke positive emotions, while references to "Rp10 juta" (ten million rupiah) create financial allure. Technical or formal terms such as "verifikasi" (verification), "rekening" (bank account), or "prosedur" (procedure) are used to give an impression of formality and enhance credibility. These technical terms reinforce the notion that the message originates from an official institution.

Syntactic Patterns

The syntactic patterns of these messages also reveal significant insights into their structure and effectiveness. Fraudulent messages often utilize direct and simple sentence constructions to minimize ambiguity and maintain clarity. However, these syntactic choices are also strategically used to reinforce urgency or to obscure potential red flags. For example, short, imperative sentences may be employed to pressure the reader into taking immediate action, while longer, more complex sentence structures might be used to mislead the victim into believing the message is genuine and well-thought-out. Common syntactic patterns identified include:

Table 5. Syntactic Patterns

Syntactic Patterns	Utterance
Imperative sentence	"Kirimkan data pribadi Anda sekarang juga!" (Send your personal data right now!)

Conditional sentence	<i>"Jika Anda tidak segera mengisi formulir ini, akun Anda akan dinonaktifkan."</i> (If you don't fill out this form immediately, your account will be deactivated.)
Complex sentence	<i>"Untuk mendapatkan hadiah Anda, klik tautan ini dan isi formulir dengan data lengkap."</i> (To claim your prize, click this link and complete the form with full information)

In imperative sentences, perpetrators often use direct commands to prompt the victim to take action. These sentences are intended to convey urgency and minimize the space for the victim to question the content of the message. Conditional sentences are used to present seemingly rational conditions. This structure exploits the victim's fear of negative consequences. Meanwhile, in complex sentences, the combination of main and subordinate clauses is used to provide detailed information while enhancing the impression of authenticity. Complex sentence structures offer step-by-step instructions that create a sense of legitimacy.

Pragmatic Aspects

The pragmatic elements of these messages involve the implied meanings and intentions behind the words. This includes how the message manipulates the victim's response, often by leveraging social norms, emotions, or trust. Fraudsters may subtly imply a sense of obligation or moral responsibility, pressuring the victim to act without considering the consequences. Additionally, pragmatic strategies such as the use of politeness, authority, and emotional appeal play a key role in establishing a false sense of trust and legitimacy. The following are some pragmatic findings.

Tabel 6. Pragmatic Aspects

Pragmatic Aspects	Utterance
-------------------	-----------

Violation of Quality Maxim	<i>"Pesan ini resmi dari Bank BRI."</i> (This message is official from Bank BRI.)
Violation of Quantity Maxim	<i>"Hadiah ini tidak memerlukan biaya tambahan, hanya verifikasi cepat di tautan berikut."</i> (This prize requires no additional cost, just a quick verification via the following link.)
Asymmetric Exploitation	<i>"Ini adalah peluang seka seumur hidup."</i> (This is a once-in-a-lifetime opportunity.)

In the pragmatic aspect of the violation of the maxim of quality, the information provided is false, such as fraudulent prize claims. The utterance in point 1 violates the maxim of quality because the information is false and is intended to deceive the victim. The pragmatic aspect of the violation of the maxim of quantity involves providing excessive or irrelevant information to divert the victim's attention. The excessive information is designed to obscure the true objective, which is to steal the victim's data. Meanwhile, the pragmatic aspect of asymmetric exploitation involves the perpetrator exploiting the victim's lack of knowledge or digital literacy. The perpetrator uses hyperbolic language to pressure the victim into making a hasty decision without careful consideration.

The linguistic characteristics in fraudulent messages demonstrate a pattern of using persuasive lexical features, syntactic structures designed to support manipulation, and violations of pragmatic principles to achieve manipulative communication goals. Lexical features like persuasive vocabulary and technical terms create urgency and trust, making the message appear credible. Syntactic patterns include simple commands and conditional sentences that pressure the victim into acting quickly or fearfully, while complex sentences enhance the message's legitimacy. Pragmatic aspects exploit the

victim's emotions and trust, violating conversational maxims to deceive, distract, and manipulate. These findings emphasize the importance of language and communication literacy in detecting signs of fraud on social media.

Comparison of Fraud Strategies on WhatsApp and Facebook

The differences in the manipulation strategies used by fraudsters on WhatsApp and Facebook are analyzed based on the communication patterns observed on each platform and are examined contrastively to understand the unique characteristics and similarities in their approaches.

Strategies on WhatsApp

On WhatsApp, fraudsters tend to employ strategies that are more personal and direct. The following are some key findings.

Tabel 7. Strategies in Whatsapp

<i>Strategi</i>	<i>Tuturan</i>
Personal and direct message	"Halo, ini dari layanan pelanggan Bank BRI. Mohon kirimkan kode OTP Anda untuk verifikasi." (Hello, this is from Bank BRI customer service. Please send your OTP code for verification.)
Creating a sense of urgency	"Anda hanya punya waktu 10 menit untuk mengamankan akun Anda." (You only have 10 minutes to secure your account)
Use of Phishing links	

Strategies involving personal and direct messages typically see fraudsters using text or voice messages that appear to be addressed directly to the victim. This strategy creates the illusion of exclusive and urgent communication, leveraging the victim's trust in institutional authority. In the strategy of creating a sense of urgency, the perpetrator exploits limited time as a means of forcing

the victim to respond quickly without careful consideration. The use of phishing links is common, with messages often including a link that directs the victim to a fake website to steal personal information. A characteristic of these links is that they often resemble official domains but with slight alterations (e.g., "bankxyz-official.com").

Strategies on Facebook

Fraud on Facebook is typically more structured, with a focus on a broader audience. The following are some strategies identified.

Table 8. Strategies in Facebook

<i>Strategy</i>	<i>Utterance</i>
Use of unreal identity	-
Mass messaging and public posts	"Selamat kepada semua anggota grup ini! Anda berkesempatan memenangkan hadiah. Klik tautan berikut untuk klaim." (Congratulations to all members of this group! You have the chance to win a prize. Click the following link to claim it.)
Exploiting visual content	-

Fraudsters use various strategies to deceive their victims. One common tactic is the use of unreal identity, where they create fake accounts to impersonate trusted individuals or organizations. Fraudsters often leverage mass messaging or public posts to reach a wide audience at once, rather than targeting individuals specifically. This strategy involves posting on social media groups, forums, or any public-facing platform where a large number of users can be exposed to the scam. By using groups or forums that appear popular or trustworthy, fraudsters can increase the likelihood of getting more victims. An example of this

strategy can be seen in the message: “Selamat kepada semua anggota grup ini! Anda berkesempatan memenangkan hadiah. Klik tautan berikut untuk klaim.” (Congratulations to all members of this group! You have the chance to win a prize. Click the following link to claim it.) The message targets all group members, providing an illusion of fairness and broad opportunity, thereby reducing skepticism. The scammer relies on the anonymity and the public nature of the platform to cast a wide net and entice a higher number of people to engage with the fraudulent offer. Additionally, fraudsters often rely on exploiting visual content, using images or logos, such as fake company branding or doctored prize documents, to give their messages a professional appearance and increase credibility, further deceiving the victim into believing the offer is genuine.

Contrastive Analysis

The comparison of strategies on both platforms reveals fundamental differences influenced by the nature of each medium.

Table 9. Contrastive Analysis

Contra- stive Pattern	WhatsApp	Facebook
Level of Personalization	Messages are more personal due to the private nature of this platform	Messages are public or semi-public with a larger audience reach.
Type of Media Used	Relies more on text and voice	Often uses visual elements such as images and videos to enhance message appeal.
Target Victim	Target tend to be more specific and individual	Targets communities or large groups

Communication Context	Tends to leverage trust in direct communication.	Perpetrators rely more on visual aspects and the size of the audience to increase success chances.
-----------------------	--	--

The contrastive analysis between WhatsApp and Facebook highlights key differences in how fraudulent messages are delivered. WhatsApp offers more personal communication due to its private nature, allowing fraudsters to target individuals with direct, tailored messages. In contrast, Facebook messages are public or semi-public, reaching a wider audience through mass posting or group messages. Regarding media use, WhatsApp relies on text and voice, making messages feel more conversational, while Facebook utilizes visual elements like images and videos to enhance the message’s appeal and credibility. The target victims also differ, with WhatsApp focusing on individuals, allowing for more specific targeting, while Facebook targets communities or large groups. Lastly, the communication context differs, as WhatsApp leverages trust in private conversations, whereas Facebook fraudsters rely on the visual impact and large audience to increase success. In short, WhatsApp is more personalized and intimate, while Facebook takes advantage of its broad reach and visual media to deceive a larger audience.

DISCUSSION

The findings of this study reveal that fraudulent messages on social media employ complex linguistic and pragmatic strategies to achieve manipulative goals. These findings support previous research which asserts that manipulative speech acts often involve violations of Grice’s (1975) conversational maxims. In the context of fraud, perpetrators often violate the maxim of quality by providing false or partially true information to build trust, as identified in studies such as Haugh (2013), which

emphasizes the importance of context in understanding pragmatic manipulation.

Lexically, the use of vocabulary such as “*selamat*” (“congratulations”), “*hadiah*” (“prize”), and “*verifikasi*” (“verification”) reflects the persuasive patterns found in Mills' (2016) research, which indicates that words with positive and authoritative connotations are frequently used in manipulative communication. This strategy aligns with Brown and Levinson's (1987) theory of face-saving, where the perpetrator seeks to protect their image as a trustworthy party while creating social pressure on the victim to act immediately.

The difference between the WhatsApp and Facebook platforms reflects the media richness theory by Daft & Lengel (2019), where perpetrators adjust their strategies based on each platform's capacity to convey messages. WhatsApp, as a private communication platform, facilitates more personal and direct messages, while Facebook allows for mass message dissemination with the aid of visual content to enhance credibility, as outlined in the study by Tandoc et al. (2018) on the effectiveness of visual-based misinformation.

This study critically departs from prior research, which has predominantly framed digital fraud as a technical or financial issue. While studies focusing on phishing mechanics or economic impact are valuable, they create an implicit tension by treating deception as a series of external events rather than an interactive, linguistic accomplishment. This overlooks a crucial dimension: the pragmatic process through which compliance is manufactured. By concentrating on the what (e.g., fake links) and not the how (e.g., the command to click it), past work has failed to explain the communicative failure at the heart of the crime. This research addresses this gap by demonstrating that technical tools are often activated by a carefully constructed sequence of speech acts. It reveals that the core vulnerability is not just a lack of digital literacy, but a susceptibility to linguistic

manipulation, a dimension largely unexamined in previous literature.

These findings enrich the understanding of pragmatic speech acts in digital communication, particularly in the context of fraud, by providing empirical evidence that perlocutionary effects, such as compliance or confusion from victims, are often achieved through the exploitation of cognitive or emotional vulnerabilities. This research extends Forgas' (2017) findings on the role of emotion in decision-making, where messages that create fear or urgency are more likely to influence the victim's actions.

Moreover, this study's primary theoretical contribution is in revealing the patterned and hybrid speech act strategies unique to digital fraud. It extends pragmatic theory by demonstrating that perpetrators do not use speech acts in isolation, but follow a "manipulation script." Specifically, the findings identify a recurring pattern where deceptive commissive acts, such as false promises, are strategically used to create a precondition of trust. This trust is then exploited to ensure the success of a subsequent directive act, like a command to send money. This research thus refines speech act theory by identifying a hybrid persuasive strategy where the illocutionary force of one act is designed to enable another. It highlights how pragmatic norms, particularly the sincerity condition of a promise, are systematically violated to achieve a perlocutionary effect of manipulation in a deceptive, non-cooperative context.

The findings offer concrete applied implications for combating digital fraud. For automated detection systems, this research provides a basis for moving beyond simple keyword flagging to more sophisticated, pragmatically-informed algorithms. These systems could be trained to recognize the specific manipulative lexical patterns and sequences identified in this study, such as the pairing of a commissive statement with a directive command, thereby flagging conversations that fit the "manipulation script." For digital literacy, the implications

are equally significant. Rather than generic warnings about scams, educational programs can be developed to teach "pragmatic awareness" as a core component of cybersecurity. These programs could use real-world examples to train users to identify the illocutionary force behind a message, helping them to recognize when they are being commanded, threatened, or deceptively promised something, thus equipping them to better resist linguistic manipulation.

Thus, this study not only supports but also deepens theoretical insights into linguistic manipulation in digital communication, while emphasizing the need for digital security approaches grounded in linguistics and pragmatics. Preventive efforts may include enhancing digital literacy to detect signs of fraud, as proposed by Rowe, M. & Lunt (2018) in the context of cybersecurity.

CONSLUSION

This study concludes that social media fraud is fundamentally a communicative and pragmatic failure, not merely a technical one. By analyzing the linguistic strategies on WhatsApp and Facebook, this research moves beyond cataloging fraud types to reveal the underlying mechanics of manipulation. The primary contribution of this work lies in identifying a replicable "manipulation script" where perpetrators systematically deploy hybrid speech act strategies, specifically using deceptive commissive acts to create false trust, which in turn ensures the success of subsequent directive acts. This finding is novel in its explicit focus on the sequential and interdependent nature of language in digital deception, a dimension largely overlooked in prior literature that has concentrated on the technical and financial aspects of fraud.

The practical significance of these findings is twofold. First, they provide a new, language-centered framework for enhancing digital literacy programs, shifting the focus from technical awareness to pragmatic resilience against manipulation. Second, they

offer a blueprint for developing more sophisticated, AI-driven fraud detection systems capable of recognizing manipulative linguistic patterns in real-time.

Future research should expand upon these insights through several avenues. Cross-platform and cross-cultural analyses could determine whether these manipulative scripts are universal or culturally specific. Further studies could also explore the integration of non-verbal cues, such as emojis and images, into these persuasive strategies. Finally, longitudinal research tracking the evolution of these linguistic tactics is essential for ensuring that preventative and technological countermeasures remain effective against the dynamic threat of online fraud.

REFERENCES

- Bank Indonesia. (2023). *Kejahatan Keuangan dalam Pembayaran Digital. Bank Indonesia.*
- Brown, P., & Levinson, S. C. (1987). *Politeness: Some Universals in Language Usage.* Cambridge University Press. <https://doi.org/10.1017/CBO9780511813085>
- Creswell, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* SAGE Publication. <https://doi.org/10.1177/1077800414557542>
- Daft, R. L., & Lengel, R. H. (2019). Organizational Information Requirements, Media Richness, and Structural Design. *Management Science*, 32(5), 554–571. <https://doi.org/10.1287/mnsc.32.5.554>
- Fatimah, Z. J. (2023). *Kejahatan Keuangan dalam Ekosistem Digital.*
- Forgas, J. P. (2017). On Feeling Good and Getting Your Way: Mood Effects on Negotiator Cognition and Bargaining Strategies. *Journal of Personality and Social Psychology*, 74(3), 565–577. <https://doi.org/10.1037/0022-3514.74.3.565>

- Grice, H. . (1975). Logic and Conversation. In P. Cole, & J. Morgan (Eds.). In *Syntax and Semantics, Speech Acts* (Vol. 3, Issue 1). Academic Press. https://doi.org/10.1163/9789004368811_003
- Haugh, M. (2013). Impoliteness and Taking Offense in Initial Interactions. *Journal of Pragmatics*, 55(10), 1–16. <https://doi.org/10.1016/j.pragma.2013.05.001>
- Kominfo. (2023). Literasi Digital dalam Mencegah Penipuan Online. *Kementerian Komunikasi Dan Informatika RI*.
- Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology*. SAGE Publication. <https://doi.org/10.4135/9789504300958>
- Lailiyah, N. (2021). Tindak Tutur Ekspresif Meminta Maaf Terpidana Korupsi di Indonesia. *Prasasti: Journal of Linguistics*, 6(1), 215.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2019). *Qualitative data analysis: A methods sourcebook (4th ed.)*. Sage Publications. [https://doi.org/10.1016/S0272-4944\(05\)80231-2](https://doi.org/10.1016/S0272-4944(05)80231-2)
- Mills, S. (2016). Discursive Approaches to Politeness and Impoliteness. *Journal of Politeness Research*, 7(2), 173–196. <https://doi.org/10.1515/jplr.2011.009>
- Putri, N., & Kurniawati, D. (2023). Analisis Modus Operandi Penipuan Digital di Media Sosial. In *UI Repository*. Universitas Indonesia.
- Rahman, A. (2023). Revolusi Digital dan Perubahan Sosial. *Media Utama*, 5(1). <https://doi.org/10.9012/mu.2023.rd.01>
- Rowe, M., & Lunt, P. (2018). Cyber Security and Identity in Online Behavior. *Computers in Human Behavior*, 85, 192–204. <https://doi.org/10.1016/j.chb.2018.03.035>
- Searle, J. R. (1969a). *A Taxonomy of Illocutionary Acts*. Cambridge University Press.
- Searle, J. R. (1969b). *Speech Acts: An Essay in the Philosophy of Language*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139173438>
- Setiadi, A. (2021). Transformasi Digital dalam Era Komunikasi Modern. *Jurnal Teknologi Dan Komunikasi*, 5(2), 45–60. <https://doi.org/10.1234/jtk.2021.5.2.45>
- Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining “Fake News”: A Typology of Scholarly Definitions. *Digital Journalism*, 6(2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
- Wijaya, R., & Sari, M. (2022). Analisis Dampak Media Sosial terhadap Pola Transaksi Digital Masyarakat Indonesia. *Jurnal Ekonomi Digital*, 3(1), 12–25. <https://doi.org/10.5678/jed.2022.3.1.12>