Studies in English Language Teaching
ISSN 2372-9740 (Print) ISSN 2329-311X (Online)
Vol. 13, No. 4, 2025
www.scholink.org/ojs/index.php/selt

Original Paper

Analysis of Fraudsters' Discourse Patterns from a Goal-adaptational Perspective

Youyue Rao[1], Bingwen Sun[2*] & Yueying Lu[3]

[1,2,3] Hubei University of Technology, Wuhan, China

[*] Corresponding author, Bingwen Sun, School of Foreign Language, Hubei University of Technology, Hubei, China

Received: October 21, 2025 Accepted: November 24, 2025 Online Published: December 4, 2025

doi:10.22158/selt.v13n4p150 URL: http://dx.doi.org/10.22158/selt.v13n4p150

Abstract

In recent years, the advancement of technology and improvement of living standards have contributed to a growing incidence of telecommunications fraud. Its impact is no longer limited to financial losses but has extended to undermining social trust and stability. Despite intensive enforcement efforts, the overall situation remains severe. Using authentic telecommunications fraud discourse as data, this study adopts Goal Adaptation Theory as its theoretical framework to analyze the discourse patterns utilized by fraudsters. The research categorizes these patterns into three types—gang-style fraud, dynamic interaction fraud and phishing fraud— and elucidates how each facilitates the achievement of fraudulent objectives. This study not only enhances public ability to recognize such frauds but also offers practical insights for raising awareness and strengthening preventive measures, thereby contributing meaningfully to fraud governance.

Keywords

Goal adaptation, fraudster discourse, discourse pattern

1. Introduction

With the improvement of people's living standards and the development of science and technology, telecommunications fraud has been increasing year by year, disrupting the normal lives of the public and threatening social safety and stability. It has become a major social hazard. Telecommunications fraud refers to criminal acts aimed at illegal possession of property, which employ various communication and network technologies to fabricate facts or conceal the truth, thereby defrauding individuals of a relatively large amount of property (Hu et al., 2016).

Currently, the methods and techniques of telecommunications fraud are continuously evolving and exhibit high concealment, which significantly complicates efforts by public security authorities to combat such crimes. Therefore, while law enforcement agencies work to crack down on criminal activities and eliminate their sources, it is equally crucial to enhance public awareness of fraud prevention. Language, as a fundamental medium for conveying information and expressing emotions, reflects the intentions and purposes of the speaker. By analyzing linguistic features, we can identify the strategies and loopholes in fraudulent discourse, thereby providing important clues for anti-fraud research. Against this backdrop, fraudulent discourse has emerged as a new research direction in discourse analysis. In-depth exploration in this area not only helps improve the public's ability to recognize and prevent fraud but also holds practical significance for curbing telecommunications fraud at the victims level.

2. Literature Review

In China, scholars have categorized fraud discourse into specific types, focusing on "immersive" anti-fraud discourse models (Liu, 2023), media-based fraudulent discourse (Bao, 2025), and SMS scam discourse (Zhang, 2025) and etc. Zhang (2025) collected a corpus of SMS scam messages and analyzed it through the lens of pragmatic identity theory. The study found that fraudsters primarily construct false pragmatic identities by appealing to economic or personal gain, typically posing as benefit inducers and false promise makers. Other scholars have examined the discourse characteristics of scammers in fraud cases, conducting studies on identity construction (Lu, 2024), discourse strategies, and discourse patterns (Yuan, 2019). Yuan (2019) employed pragmatic presupposition theory to analyze discourse patterns in telecom fraud cases, identifying four categories: gang-style, designed, phishing, and dynamic interaction patterns. Based on the motives and objectives of the perpetrators, five discourse strategies were identified: linguistic disguise, linguistic imitation, linguistic traps, linguistic probing, and linguistic truth-telling. Domestic research on fraudulent discourse thus begins with the classification of discourse types and further explores their distinctive features.

Internationally, Olajimbiti (2018) applied Halliday and Hasan's Generic Structure Potential and an aspect of Fetzer's cognitive context model, identifying six typical discourse patterns: salutation, discourse initiation, enticing information, mild conscription into business, request and subscription. He found that online scammers adopt patterns and contexts similar to those used in traditional fraud, employing persuasive language to deceive potential victims. Hiss (2015) explored how scammers use linguistic strategies in fraudulent emails to shape a sense of identity and establish interactive relationships with recipients. By incorporating cultural indexicals, interactional roles, and narrative strategies, scammers reinforce identity claims through cultural cues, blend fictional content with real contexts via interactive roles, and use e prototypical elements from traditional fairy tales to build connections. Chen (2020), from a discursive psychology perspective, used conversation analysis to examine threatening language features in Chinese mobile phone scam dialogues. He pointed out that scammers construct false identities by alternating between information gaps and information sharing in turn-taking dialogues, supplemented

by threatening tonal techniques such as repetition, interruptions, raised pitch, and increased volume to induce panic in victims.

In summary, given the intrinsic characteristics of the cases used in this study and considering the overlapping nature of the discourse pattern classification proposed by Yuan (2019), this paper chooses to conduct analysis from the perspective of Goal Adaptation Theory. The study will focus on how fraudsters, within the three discourse patterns—gang-style, dynamic interaction, and phishing—make linguistic choices to achieve their fraudulent goals, and further analyze how these discourse patterns dynamically adapt to the physical, social, and psychological worlds in context.

3. Goal-driven Fraudsters' Discourse Patterns

3.1 Gang-style Fraud

In telecommunications fraud, the gang-style discourse pattern exhibits a high degree of "role-playing" and "scripted" characteristics. Criminal groups assign specific roles to members through internal division of labor, supported by tailored dialogue scripts, forming an interlocking system of deception.

Example 1: (Aunt Wang receives a call one day from someone claiming to be a police officer)

Aunt Wang: Can you say my ID number again? I've got my ID right here. Just read it to me.

Fraudster 1: If you won't cooperate, just hang up. I'm done talking. Hang up now! Why is this so hard to understand?

Aunt Wang: I didn't get much schooling, and I've never really left home.

Fraudster 1: Then do exactly as I say. Let me ask you: Can you go to the Changsha Public Security Bureau to get evidence? Go now!

Aunt Wang: I can't go. I never go out. I can't make it there.

Fraudster 1: Since you can't go, like I said, I'll transfer you to Changsha Public Security Bureau. You're involved in a case—a Bank of China card under your name was used in a crime. The Changsha police need you to help prove you didn't get that card. Got it? That's the only way you won't be blamed. If you don't help find the evidence, they can freeze all your money, properties, and bank accounts. If you agree to the freeze today, you don't have to do anything. Yes or no?

Aunt Wang: Of course not.

(Voice prompt: Hello, transferring you to the Changsha Public Security Bureau branch.)

Fraudster 2: Hello, Changsha Public Security Bureau. How can I help you?

Aunt Wang: I just got a call about some case?

Fraudster 2: This is a confidential case we're handling. There are over 200 people involved. Hold on, the officer in charge is here—I'm just a staff member. Wait a moment.

(Another fraudster posing as an officer takes the call)

Fraudster 3: Hello, madam.

Aunt Wang: Hello, sir.

Fraudster 3: Let me confirm: were you born April 1, 1976? Is that you?

Aunt Wang: Yes.

Fraudster 3: That matches. Today, our Changsha Bureau asked Yaocheng police to inform you that you're involved in this case. Understood?

Aunt Wang: Understood.

Fraudster 3: Here's the situation: We've cracked a major case led by a criminal named Liu Ju. This is Officer Chen, and I need to ask you a few questions about the case. Answer honestly. Also, this is an investigative line—we can't talk long. I, officer Chen, will hang up and send you a WeChat voice message. Remember: after we hang up, don't use your phone. Don't make or take any calls. Clear?

In this case, Aunt Wang fell victim to a coordinated, gang-style discourse pattern. The fraudsters constructed three interlocking false identities: an "officer from the Yaocheng City Public Security," a "staff member at the Changsha Public Security Bureau," and finally "Officer Chen." This carefully orchestrated sequence allowed the scam to progress in a stepwise manner.

The overarching goal was to gradually gain the victim's trust and ultimately achieve the fraudulent objective. The first impersonator, posing as the "officer from Yaocheng City," guided the victim to explain the reason for the call and established a contextual background for subsequent steps. His core function was to build initial trust and transfer the call to the next accomplice, thereby paving the way for the formal execution of the fraud. By adopting a stern tone, the fraudster adapted to the psychological world of the victim, instilling fear and leveraging her desire to prove her innocence. Subsequently, the "staff member of the Changsha Public Security Bureau" and "Officer Chen" collaborated to fabricate a scenario in which the victim "encountered the investigating officer at the police station," thereby enhancing the overall credibility through situational simulation. Here, the verbal tactics adapted to the physical world by constructing a false setting of a police bureau. The impersonated "Officer Chen" frequently used self-referential expressions such as "I, Officer Chen, will…" throughout the dialogue. Through linguistic repetition, he reinforced his false identity, deepened the victim's recognition of his "police officer" role, and thereby strengthened psychological control.

3.2 Dynamic Interaction Fraud

The dynamic interaction fraud is highly dynamic. Based on the victim's personal information, the fraudster engages in highly interactive communication, continually adjusting, selecting, and combining different verbal tactics to craft a targeted and deceptive script designed to mislead the victim. This pattern includes two distinct approaches: the adaptive approach and the pre-set approach. The adaptive approach relies on fabricating "coincidences" to extract the victim's real-time information, allowing the scammer to adjust and deceive accordingly. In contrast, the pre-set approach involves laying traps or schemes in advance, forcing the victim into a closely guided sequence of actions (Yuan, 2019).

(Mr. Wang receives a call from someone claiming to be an ICBC customer service agent.)

Fraudster: Hello, this is ICBC customer service, ID 12345. Our system picked up a suspicious transaction on your card this morning—5,000 RMB, from another city, at 10:15 AM. Was that you?

Mr. Wang: No, that wasn't me! I've been home all day. I didn't make any payment.

Fraudster: I see—your account might be at risk. To keep your funds safe, we'll need to confirm your identity now. Can you give me your full name and ID number?

Mr. Wang: It's Wang Wu. My ID number is X.

Fraudster: Thanks. We do see some risk on your account now. To secure it, we'll need you to help with a quick security check. Please tell me your bank card number and the amount of your last transaction. We'll send a verification code to your phone—make sure not to share it.

Mr. Wang: My card number is X. Last time I used it was yesterday at the supermarket—100 RMB.

Fraudster: Got it. We've noted that. To fully protect your account, you'll need to *log into our security page* right now and follow the steps. Just so you know, this is time-sensitive—if you don't act within 30 minutes, your account will be frozen.

Mr. Wang: So what do I need to do?

Fraudster: Click the link I'm sending you. Then *enter your card password and the verification code* you receive. We'll move your funds to a protected account temporarily and return them after everything's cleared.

In the present case, the fraudster strategically deployed both the adaptive approach and pre-set approach with the fundamental goal of deceiving Mr. Wang into transferring his funds to a so-called "secure account," thereby accomplishing financial fraud. The fraudster first deployed the pre-set approach by establishing a fabricated scenario, claiming that a suspicious transaction had occurred in a different city using Mr. Wang's bank card. This predefined trap served a dual function: first, to construct an authoritative persona and gain the victim's trust, and second, to pave the way for subsequently extracting personal information.

When Mr. Wang denied conducting the transaction, the fraudster dynamically shifted to the adaptive approach, seizing the opportunity to request key details such as his full name and ID number. Based on the victim's responses, the scammer adjusted the fraudulent strategy in real time. Subsequently, through a series of directive utterances—such as "please log in to the security page," "enter your bank card password," and "provide the verification code"—the fraudster systematically guided Mr. Wang through a predetermined sequence of actions. This carefully orchestrated, step-by-step discursive progression led the victim, often unknowingly, deeper into the trap, ultimately resulting in financial loss.

3.3 Phishing Fraud

The phishing fraud represents one of the most prevalent modes of communication in the initial stages of telecommunication fraud. Criminal groups utilize automated tools to disseminate fraudulent information on a large scale through channels such as SMS, social media groups, and pop-up web pages. The core logic of this pattern lies not in precisely targeting specific individuals, but in casting a wide net to filter out those who respond with panic, actively reply, click on embedded links, or call designated numbers. The phishing-based discourse pattern is characterized by a high degree of scripting and automation.

Example 3: (The following message was sent by a fraudster posing as a university teacher in a course group, accompanied by the scammer's Alipay QR code.)

Class notice: We're arranging the required Huanggang study materials for this semester. Deadline: April 21. Delivery next Friday. Cost: 60 RMB. Please pay using the Alipay QR code below. After paying, post your receipt in this group for my records. First 5 students to pay get a water bottle and pencils. Thank you!

In this case, the fraudster did not target specific students but rather broadcasted a false notification within the group chat, aiming to exploit those who responded proactively. The content of the message revolved around the theme of "ordering tutorial and learning materials," with language deliberately crafted to mimic an instructor's tone, thereby leveraging the inherent trust in teacher-student relationships and the specific social context of a group chat.

Due to the spatial disconnect inherent in online interactions, victims find it difficult to verify the identity of the sender in real life. The fraudster capitalizes on this by constructing the identity of a "university teacher" through fabricated profile pictures, display names, and speech patterns, thereby luring the victims into lowering their guard and proceeding with the transfer. This case serves as a critical reminder that when encountering various types of online information, it is essential to remain vigilant and exercise careful judgment. Even if the sender appears to be a "familiar person," one should verify their identity through multiple channels before making any transfers and refrain from trusting unverified information.

4. Conclusion

Guided by the framework of Goal Adaptation Theory, this study examines the discourse patterns employed by fraudsters in telecommunications scams, with a focus on the underlying intentions of their discourse pattern and the dynamic adaptation mechanisms to multiple contextual dimensions. Through the analysis of authentic cases, the study identifies three typical fraud discourse patterns: group-based, menu-based, and phishing-based, revealing how each is driven by and serves specific fraudulent objectives. Furthermore, from the three dimensions of the physical, social, and psychological worlds, it elucidates how scammers strategically align their linguistic choices with contextual factors to achieve their deceptive ends. Based on the findings, this paper proposes practical preventive recommendations: when encountering suspicious information, the public should remain vigilant and refrain from credulity, protect personal information from disclosure, firmly avoid transferring funds, and proactively verify through multiple official channels. These measures are intended to enhance the public's ability to recognize and resist telecommunications fraud.

References

Bao, Y. L. (2025). Media Discourse Analysis of Telecom Network Fraud in "Legal Daily". *Voice & Screen World*, (05), 29-31. (in Chinese)

Chen, J. (2021). "You are in trouble!": A discursive psychological analysis of threatening language in Chinese cellphone fraud interactions. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *34*(4), 1065-1092.

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

Hu, J. Y., Liu, H. Y., & Cai, D. Q. (2016). Research on Telecom Fraud Crimes and Prevention Technologies. *POLICE Technology*, (02), 4-7. (in Chinese)

Liu, L. W. (2023). *Research on the Construction of "Immersive" Anti-fraud Discourse Model* (Master's thesis, People's Public Security University of China). CNKI. https://doi.org/10.27634/d.cnki.gzrgu.2023.000239. (in Chinese)

Lu, J. X. (2024). *Pragmatic Identity Construction and Strategies in Telefraud Discourse* (Master's thesis, Guangxi Normal University). CNKI. https://doi.org/10.27036/d.cnki.ggxsu.2024.001914. (in Chinese)

Olajimbiti, E. O. (2018). Discourse pattern, contexts and pragmatic strategies of selected fraud spam. *Crossroads. A Journal of English Studies*, 02(21), 53-63.

Yuan, Y. (2019). Research on Discourse Patterns and Speech Strategies in Telecom Fraud Cases. *Journal of Guizhou Police Officer Vocational College*, *31* (04), 64-68. https://doi.org/10.13310/j.cnki.gzjy.2019.04.010. (in Chinese)

Zhang, Y. C. (2025). A Study on SMS Fraud Discourse in China from the Pragmatic Identity Perspective. *International Journal of Language, Culture & Law*, (01), 102-116. (in Chinese)