Advances in Social Science and Culture
ISSN 2640-9682 (Print) ISSN 2640-9674 (Online)
Vol. 7, No. 3, 2025
www.scholink.org/ojs/index.php/assc

Original Paper

A Pragmatic Analysis of the Manipulative Discursive Mechanisms in Cyber Frauds

Chen Meisong[1]

[1] School of Liberal Arts/Centre for Singapore Studies, Nanjing University of Information Science & Technology

Fund Project

This study was supported by the Project of Social Science Foundation of Jiangsu Province (grant no. 21YYB001), the Project of Philosophy and Social Science Research in Colleges and Universities in Jiangsu Province (grant no. 2021SJA0156), and by the Institute of National and Regional Culture, Nanjing University of Information Science & Technology.

Received: February 24, 2025 Accepted: April 15, 2025 Online Published: June 23, 2025

doi:10.22158/assc.v7n3p121 URL: http://dx.doi.org/10.22158/assc.v7n3p121

Abstract

Cyberspace is pivotal for national security and economic development, yet pervasive cyber fraud poses significant threats to societal progress. Through a pragmatic lens, this study reconceptualizes cyber fraud as a strategic discursive manipulation wherein perpetrators systematically violate communicative norms to exploit cognitive biases. Drawing on real cases, this study identify and analyze its triadic discursive nature which includes dependency on convenient virtual channels enabling rapid, wide dissemination, contradictory double communicative intentions masking self-serving motives beneath a veneer of altruism or mutual benefit; and exploitation of alluring discourse leveraging cognitive biases through inducements to bypass rational scrutiny. This pragmatically grounded analysis reveals how fraudulent discourse actively corrodes networked communication contexts, inflicts multifaceted harm on netizens, and misappropriates language resources. Consequently, we argue that effective countermeasures necessitate discursive governance, implemented through three key dimensions: regulating platform-based communicative behaviors, deploying counter-discourse campaigns and establishing language standardization frameworks. This analysis, grounded in the Chinese context, offers a linguistically-informed approach to combating cyber fraud with potential cross-cultural relevance.

Keywords

cyber fraud, discursive nature, pragmatic manipulation, online communication, discourse governance

1. Introduction

Cyber fraud has become a pervasive global challenge, posing significant threats to both individual economic security and the trust foundation of the digital environment. A survey in 2024 showed 3.2 million fraud incidents in the UK, which is yet significantly underreported (Note 1). In the USA, fraud reports accounted for 2.6 million, making up 48% of all consumer reports (Note 2). In China, the situation is equally alarming. The China Internet Network Information Center (CINIC) reported in 2022 that 16.4% of Chinese netizens had been victims of cyber fraud (Note 3). These statistics underscore the severe and urgent nature of the problem. In view of the fact that online fraud is mostly realized with the help of language, a basic tool of human communication, and often adopts fixed speech "routines" (Cui et al., 2018, p. 33). From a pragmatic perspective, we conceptualize cyber fraud as strategic communicative manipulation. Fraudsters systematically violate conversational norms while dynamically adapting to victims' cognitive environments, exploiting language's inherent manipulability to achieve illicit gains. This approach may illuminate the cognitive-pragmatic underpinnings of fraudulent discourse.

2. Defining Cyber Fraud

The progress of Internet technology has profoundly changed the traditional way of people's work and life, significantly affecting all aspects of Chinese people's private and public affairs (Ren, 2018). While bringing convenience to people, it has also become a fraud tool and protective cover for criminals. Cyberfraud is a negative pragmatic phenomenon in which false information is transmitted through language representation with the help of network technology, so as to seek the interests of some individuals or minorities with ill intentions. The implementation and dissemination of cyber fraud cannot be separated from some important components, including convenient communication channels, contradictory double communicative intentions, and alluring discursive contents.

To comprehend the discursive nature of cyber fraud, it is essential to first clarify the concept of "fraud" itself. Lexicographical definitions, academic literature, and search engine results reveal that terms semantically akin to "欺诈" (fraud, qīzhà) include "诈欺" (zhàqī) and "诈骗" (zhàpiàn). These terms share a common context where one party, driven by malicious intent, employs deceptive means to induce erroneous perceptions in another party (an individual or a group of people), thereby prompting improper financial or material decisions.

Firstly, "qīzhà" (欺诈) vs. "zhàqī" (诈欺). Dictionary definitions treat these two terms as interchangeable. For instance, the "Chinese Dictionary" (《汉语大辞典》) defines qīzhà" as deceiving others through cunning and dishonest tactics while "zhàqī" is defined as fraudulent deception (see "Chinese Dictionary" online edition: Note 4). Similarly, "shuōwénjiězì" (Analytical Dictionary of

Characters, “说文解字”: Note 5) interprets “诈” (“zhà”) as to deceive. In academic discourse, scholars seldom distinguish between “qīzhà” and “zhàqī” when analyzing related phenomena. However, debates on legal terminology precision suggest that “zhàqī” is more appropriate as a formal legal term, whereas “qīzhà” represents its colloquial counterpart (Chen & Chao, 2005). Consequently, for the purpose of examining linguistic practices in societal contexts, this study treats “qīzhà” and “zhàqī” as synonymous, collectively referred to as “fraud”. Secondly, “qīzhà” (欺诈) vs. “zhàpiàn” (诈骗). The term “zhàpiàn” (诈骗) is predominantly used in legal contexts to denote criminal acts and corresponding criminal penalties. According to Article 266 of China’s “Criminal Law”, the crime of fraud refers to the act of illegally appropriating public or private property through fabricated facts or concealed truths, with penalties ranging from detention to fines depending on the severity of the offense. In broader humanities and social science research, online fraud encompasses any behavior that exploits digital tools or platforms to secure illicit gains, including both severe criminal offenses such as large-scale financial fraud) and pervasive non-criminal deceptions such as false advertising, deceptive marketing.

With all these understandings in mind, we deem that the concept of “fraud” (“qīzhà”) in this study carries a more expansive semantic scope than the strictly legal definition of “zhàpiàn”, encompassing both criminal and non-criminal deceptive practices. For consistency, this research employs “fraud” as an umbrella term integrating “qīzhà” and “zhàpiàn”. Cyber fraud constitutes a negative pragmatic phenomenon where false information is transmitted through digital language representation to secure illicit benefits. This phenomenon essentially manifests through interrelated mechanisms such as strategic violations of conversational norms, cognitive manipulation via induced biases, and contextual reframing to create false urgency, which enable perpetrators to circumvent victims critical evaluation.

3. Discursive Features of Cyber Fraud

3.1 Convenient Disseminating Channels

According to CNNIC’s 53th report (Note 6) issued in December 2023, the scale of Chinese Internet users for 1.092 billion, the Internet penetration rate of 77.5%. Internet applications include basic applications, business transactions, network entertainment and public services, which virtually cover all aspects of People’s Daily work and life needs. Non-netizens who do not go online will face various inconveniences such as the difficulty of reducing services at offline service outlets, the inability to obtain information in time, the inability to pay in cash, and the inability to buy tickets and hang up numbers. It can be imagined that the scale of Internet users will continue to expand in the future, and people will be more dependent on the network.

The convenience and virtuality of the Internet make the network communication platform also become a fast channel for the spread of cyber fraud messages. First of all, the network-based information production mode breaking through the limitations of time, space and cost has diversified information sources, and can realize the rapid network communication of all netizens to all netizens. Because of this, the number of audiences involved in online fraud far exceeds the coverage capacity of traditional media.

The multiple communication channels of cyber fraud mainly include in China microblog, wechat, blog, QQ and other instant chat tools, as well as network forums, virtual network communities, E-mail and so on. These communication channels have some similarities in the communication mode, such as fast information transmission speed and wide influence range, and there is a close linkage between different communication channels, which provides technical support and practical possibility for the rapid dissemination of cyber fraud information. Secondly, the network world is a high-tech virtual space, and network communicators generally do not need to face real communication objects. Scholars point out that the Internet is a virtual space for constructing identities, which lacks many constraints of realistic communication, so communicators can construct multiple identities according to their own needs to a large extent (He & Chen, 2015), and even commit fraud through false identity construction (Chen, 2013, pp. 64-78). Although most communication platforms require real identity authentication (such as Weibo, Tencent QQ, wechat, etc) with the increasing management of network behaviors, the authentication procedures are not impeccable, and identity theft and account theft occur from time to time. Pragmatically, this environment permits breaches of Grice's Relation Maxim (Grice, 1975), as fraudsters deploy contextually irrelevant narratives that would raise suspicion in face-to-face communication but flourish in fragmented computer-mediated exchanges.

3.2 Contradictory Double Communicative Intentions

Interpersonal communication usually revolves around specific communicative goals and is carried out with the help of certain linguistic means and pragmatic strategies. In this process, the communicator tries to make the other person understand him or her and tries not to mislead him or her. However, there may be power oppression, social prejudice, fraud and other behaviors behind language use (Chen, 2013).

On the surface, fraudsters appeal to the affective factors of the audience, such as emotions, preferences, needs and interests, explicitly give the listener the right to participate, and carry out false relationship management (Chen & Chen, 2020). In fact, the real motive is to seek personal gains, which reflects the mismatch between the surface and real communicative purposes, and is a deviation from the traditional discourse rules. Stealing instant messaging accounts such as wechat, Tencent QQ to commit fraud is a common form at present. In typical cases, the thief asks the recipient to "help" with the transfer, which is used to help pay for the medical expenses of relatives and friends who have had an accident. On the surface, for the benefit of a third party, the speaker asks the recipient to act with him, which is a friendly act of sincere help to a friend, but in fact it is a money fraud under the cover of a fictitious good deed. Fraudsters often also meet the direct interests of the recipient as the surface intention, such as informal recruitment websites published part-time information "teach you a way to earn more than ten thousand yuan per month online, mobile phone at home can do part-time", with simple operations and monetary interests to attract the recipient. As is substentiated in these cases, it can be seen that fraudsters have dual communicative intentions, a claimed altruistic purpose versus a concealed self-serving agenda. These intentions, while distinct, operate interdependently; fraudsters deliberately

select linguistic units and pragmatic strategies that foreground purported altruism to mask underlying self-interest. In such cases, the surface discourse promotes collective benefit, e.g., “helping” others gain income, yet the ultimate objective remains unilateral gain through victim persuasion. This fundamental mismatch, even contradiction, between professed and actual aims epitomizes the two-skinned nature of fraudulent communication. Pragmatically speaking, fraudsters perform Leech’s (1983) Sympathy Maxim to simulate altruism superficially, while in fact they violate Grice’s (Grice, 1975) Quality Maxim through fabricated scenarios.

3.3 Alluring Discourse

Language information is one of the sources for communicator impression management and relationship management (Zhou et al., 2014; Ye & Zhao, 2022), and text is the preferred medium in network communication and the main data type (Carlson et al., 2004). In the event of fraud, the communicative party usually processes the key information through linguistic means, and the key to transmitting false information and achieving the intention of fraud lies in the leading discourse.

As the constituent element of the cyber fraud, the leading discourse is embodied in the fraudulent behavior from two different angles of “benefit” and “harm”. On the one hand, the cyber fraud often takes the benefit as the bait, infects the cognition of the speaker and affects his judgment. Fraudsters often take the addressee's ability to obtain benefits, goods or money, as the basis of discourse to achieve their purposes of persuasion and fraud (Horvitz & Pratkanis, 2002; Gragg, 2003). Despite the obvious risks, there are still large numbers of seemingly rational people who fall for the scam and lose their savings. The network space is full of various temptations, such as winning well-known enterprises or entertainment programs, exchanging points, lowering prices, rewards, heavy money, high-salary recruitment, etc., network communication will fall into these interest traps if you are careless. It can be seen that fraud based on inducement of profit can be widely successful (Harrison et al., 2016). On the other hand, fear appeal has become an effective persuasive discourse strategy for fraudsters in cyber fraud. Fraudsters incite fear by fabricating “dangerous” situations or “serious” consequences. In the major fraud case of peddling fake and inferior health care products uncovered by Chongqing police in 2022 (Note 7), criminal gangs simultaneously promote product efficacy while employing threats regarding personal credit exposure, privacy breaches, account freezes, insurance cancellations, or legal shields to coerce victims into purchasing refused and inferior products.. Such cases include reminding the recipient of suspected “money laundering” due to the theft of identity information through wechat and other means, threatening the recipient with edited “pornographic photos”, and having to browse their wanted notices or arrest warrants online. Such messages that imply very serious consequences often cause the recipient of the message to experience a negative emotional state (Petty et al., 2001), making them cognitively inclined to agree with the message and to take preventive or self-protective risk avoidance measures (Fishbein & Ajzen, 1975).

4. The Negative Impact of Cyberspace Fraud

Fraudsters rely on network platforms, take language as a tool and sacrifice the rights and interests of others as the premise to seek improper or even illegal interests for themselves, which damages the civil and healthy development of network communication context, endangers the property safety, rational cognition and legitimate rights and interests of the potential or actual victims, and is a serious form of language disorder.

4.1 On the Context of Network Communication

Context is the environment that interpersonal discursive communication depends on. It determines the characteristics of discourse communication and has an important influence on it. And discursive communication also reacts to the social environment. The Internet environment has greatly enriched the content of human life and improved the efficiency of interpersonal interaction. However, advanced network technology and convenient network communication platform provide the communicative context for criminals to commit language fraud, and become the soil for breeding cyber fraud which erodes pragmatic trust, the fundamental expectation of sincerity and ethical intentionality in the computer-mediated communication environment.

First, fraudsters seek improper or even illegal interests of a few people through advanced virtual communication platforms, which deviates from the original intention of scientific and technological development and is a disharmonious note of human civilization. Scientific and technological progress is to serve the needs of the majority of people and promote the development of civilization and social progress. Modern computer technology has set up a new virtual communication environment for interpersonal interaction, especially breaking through regional restrictions, so that network communication has the characteristics of swiftness. This new mode of communication can promote active information transmission and positive emotional interaction. The diversified network communication platforms represented by instant messaging tools effectively meet people's various needs in collaborative office work, interpersonal relationship maintenance, home-school communication, and government information release. However, the network communication platform is also used by the ill intentioned few, and has become the parasitic place and the core element of the cyber fraud. From the statistical analysis of related fraud events (Note 8). QQ and wechat are the most commonly used communication methods for fraud implementation at present, and the number of fraud incidents involved accounts for 73.8% and 24% of the total number of fraud incidents, respectively, the vast majority of which are cross-platform fraud implemented by telephone and wechat, QQ and other Internet applications at the same time. Fraudsters who are motivated by profit take advantage of the development of technology to seek personal gains by cheating, and deviate from the normal track of the civilized world.

Second, cyber fraud involves many topics and fields, disrupting the normal order of network communication, forming trust and moral crisis, which is not conducive to social progress and national development. Chinese culture takes "honesty" as its core concept, "honesty" as its foundation, and "no

deception" as its first principle. As recorded in the Doctrine of the Mean (《中庸》), Sincerity is the way of heaven, and sincerity is the way of man, and the principle of sincerity has universal value. At the same time, ethical pragmatics also points out that the ethical dimension should be attached importance in verbal communication, believing that discourse communication can reflect the moral order and involve moral and ethical issues (Chen, 2017). Online frauds shows "inclusiveness" in the distribution of topics, involving all aspects of people's study, work and life. In terms of communication intention and communication strategy, it completely deviates from the cooperative attitude that should be followed in normal communication, subverts the healthy relationship between rights and obligations, abandones the principle of "sincerity" advocated by Chinese culture, and ignores or even challenges the moral order. The frauds pretending to be relatives and friends produces "acquaintance" panic among people, and network communicators have to be cautious when involving sensitive property and private information, and interpersonal trust is weakened. The credibility of enterprises, institutions and professionals being affected, the public tend to think twice about the recommendations and certifications from authoritative institutions or experts. Taking vulnerable groups such as minors and the elderly as key groups, taking advantage of their cognitive defects or emotional needs, and using the name of "respecting the old and loving the young" to "trap the old and harm the young" is contrary to ethics and morality. It is not difficult to imagine that all kinds of cyber fraud make it difficult to distinguish right from wrong, true and false, and have caused widespread trust crisis and moral crisis, affecting social stability and national development.

4.2 On Netizens

In the Internet age, anyone can be a victim of fraud. Cyber fraud misleads the rational cognition and behavior of the Internet users, bringing a wide range of property losses, psychological damage and cognitive disorders.

First of all, cyber fraud causes property losses, mental damage and even life safety to the direct victims. According to the China Network Integrity Development Report released by the China Federation of Network Social Organizations (Note 9), most of China's Internet users have encountered online fraud to varying degrees. 12.9%, 27.1% and 35.5% of respondents said they had often, sometimes and rarely experienced online fraud, respectively, while only 24.5% said they had never experienced such fraud. Cyber fraud cases not only affect the consumption experience, but also may bring great property and security threats, causing extremely bad effects in society. Fortunately, the police continue to crack large "network card" fraud gangs, large "network dating" fraud gangs, large network fraud money laundering gangs and other cases. However, the staggering number of suspects, the amount of money involved, and the number of victims across the country reflect the enormous factual harm and potential threat that various cases of cyber fraud have caused to the vast community of online communicators.

Secondly, cyber fraud sets pragmatic traps and causes cognitive impairment. The Internet era has brought about a major change in consumption behavior, whether it is material consumption or information consumption, people's dependence on the Internet is unprecedented. Data show that

China's online shopping accounted for more than 80% of users in the Internet (Note 10). However, online advertising fraud brings great cognitive impairment and difficulty in choice to online consumers. In today's popular medical beauty, fraudulent propaganda from medical beauty companies and even maternal and child health care hospitals disturbs the order of the medical beauty market, seriously misleads the consumption intention of medical patients, and infringes on their legitimate rights and interests. At a time when the global epidemic was raging, the prevention and control of the epidemic was the responsibility of every citizen, and the whole country needed to work together and fight side by side. However, fraudsters exploit pandemic concerns through various "clever" tactics, such as impersonating epidemic coordinators, vaccination surveyors or health authorities; promoting fraudulent nucleic acid tests, COVID-19 treatments/vaccines, or epidemic-material investments; fabricating refund schemes for pandemic-related items. These deceptions actively undermine public adherence to legitimate epidemic prevention norms and behaviors. While the cyber fraud targeting minors has a negative impact on their cognition, it will also twist their world view, values, outlook on life and other aspects.

Moreover, cyber fraud threatens the security of personal information and brings communication panic. Cyber fraud mostly involves the disclosure of identity information. On the one hand, Internet users must do everything possible to take protective measures to ensure the security of personal information. A variety of anti-virus software, protection programs, authentication methods came into being. These measures effectively protect the security of personal information to a certain extent, but also reflect the general lack of security and security panic in network communication. On the other hand, whether the identity of the other party is true and whether the source of information is reliable is also a problem that network communicators have to consider often, which becomes a barrier for harmonious interpersonal communication. As mentioned in the anti-fraud propaganda, "You may not have been deceived. It is not because you are smart or lucky. The only reason is that the customized script for you is still on the road", it can be seen that the cyber fraud threatens everyone, and it is easy to produce people's self-defeating communication panic.

4.3 On language Resources

Spoken and written language is the most important communication tool and information carrier of mankind, the basic element and distinctive symbol of culture, and an important force for promoting historical development and social progress. The language used in network communication should reflect its public welfare attributes, serve the majority of people, and play a positive role in historical and cultural inheritance, social and economic development, national quality improvement and other aspects. Cyber fraud takes language as a fraud tool, which is a serious expression of language anomia, reflecting the negative or improper use of language, touching the pollution-free bottom line of language ecology, and showing a bad impact on language in terms of communicative purposes, use strategies and communicative effects.

First of all, cyber fraud reflects a serious deviation from language norms concerning the purpose of

communication. Social development in the new century needs to pay attention to the standardization of language at the social level, which is related to "right and wrong, good and evil, beauty and ugliness" (Liu, 2019). However, in the guise of thinking for others, fraudsters disregard laws, morals and ethics, and use language resources as a means to seek improper or illegal benefits. Secondly, cyber fraud shows the serious misuse of language in the language use strategy. Cyber fraudsters use exaggeration, repetition, borrowing and other techniques to invoke various resources to form negative language memes such as "story books" and routines of fraud, which can be quickly copied and spread. Moreover, cyber fraud has seriously damaged the language function in terms of communication effect. Cyber fraud brings material and spiritual damage to individuals, affects social atmosphere and public opinion, endangers national stability and development, and violates the fundamental principle that language should serve human progress.

5. Conclusion

Cyber fraud, as a discursive-performative crime, exploits linguistic strategies to manipulate victims through fabricated altruism, fear appeals, and identity deception. This study establishes cyber fraud as a negative pragmatic phenomenon in which fraudsters operationalize Gricean violations and strategic politeness within a deceptive pragmatic framework adapted to victims' cognitive vulnerabilities. This study delineates its tripartite discursive nature, channel dependency on virtual platforms for rapid dissemination, contradictory intentionality masking self-interest under claims of mutual benefit, and exploitative discourse weaponizing cognitive biases to bypass rational scrutiny. These mechanisms severely corrode three dimensions of sociolinguistic ecology, networked communication contexts for eroding trust in digital public spaces, netizen agency forcausing financial, cognitive, and psychological harm, and Language resources for normalizing deceptive pragmatics as "acceptable" memes. Consequently, we believe that countermeasures must prioritize discursive governance in behavioral regulation of platform-based speech acts, anti-fraud discourse campaigns deconstructing manipulative linguistic routines, and language standardization frameworks penalizing deceptive pragmatics in public communication. While this study centers on Chinese cyberspace, its theoretical lens of bridging ethical pragmatics, criminology, and discourse analysis may offer cross-cultural applicability. Future research may quantify linguistic coercion efficacy across demographics and expand corpus-based deception typologies. Only through sustained interdisciplinary collaboration can we dismantle fraud's discursive infrastructure.

References

Carlson, J. R., George, J.F., Burgoon J K, et al. (2004). Deception in computer-mediated communication. *Group Science & Negociation*, *13*(1), 5-28. https://doi.org/10.1023/B:GRUP.0000011942.31158.d8

Chen, D., & Chao, Z. X. (2005). On fault and deceit: Comments on popularization of legal language.

Academic Research, *2005*(8), 67-73.

Chen, M. S., & Chen, X. R. (2015). A pragmatic analysis of mock rapport management: With evidence from online rumors. *Foreign Languages in China*, *17*(06), 41-47.

Chen, X. R. (2013). *Critical Pragmatic Studies on Public Discourse*. Shanghai: Shanghai Foreign Language Education Press.

Chen, X. R. (2017). Cutting-edge interdisciplinary research: Ethical Pragmatics. *Foreign Languages in China*, *77*(3), 9-10.

Cui, M., Ouyang, G. L., & Hu, Y. B. (2018). *Interpretation of the Discourse Pattern of Telecom fraud*. Beijing: Xinhua Publishing House.

Department of Language Application Administration of the Ministry of Education. (2013). *Outline of the National Medium and Long Term Language Reform and Development Plan* (2012-2020)[M]. Beijing: Language Press, 2013: 1.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behaviour: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Gragg, D. (2003). *A multi-level defence against social engineering*. Bethesda, MD: SANS Institute,.

Grice, H. P. (1975). Logic and conversation. In P. Cole, & J. Morgan (Eds.), *Syntax and Semantics* (Vol. 3). New York: Academic Press.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, *40*(2), 265-281. https://doi.org/10.1108/OIR-04-2015-0106

He, H., & Chen, X. R. (2015). A pragmatic account on the construction of online shop owners' relational identities. *Modern Foreign Languages*, *38*(3), 347-438.

Horvitz, T., & Pratkanis, A. R. (2002). A laboratory demonstration of the fraudulent telemarketers'1-in-5 prize tactic. *Journal of Applied Social Psychology*, *32*(2), 310-317. https://doi.org/10.1111/j.1559-1816.2002.tb00217.x

Leech, G. N. (1983). *Principles of Pragmatics*. London: Longman.

Liu, C. Q. (2019). The view of linguistic specification today: Impartial and harmonious, honesty and pursuing elegance. *Journal of Jiangxi Normal University(Philosophy and Social Sciences Edition)*, *52*(6), 68-75.

Petty, R. E., DeSteno, D., & Rucker, D. D. (2001). The role of affect in attitude change. In J. P. Forgas (Ed.), *Handbook of Affect and Social Cognition* (pp. 121-236). Mahwah: Lawrence Erlbaum Associates.

Ren, W. (2018). Exploring Chinese digital communication. *Discourse, Context & Media*, *26*(11), 1-4. https://doi.org/10.1016/j.dcm.2018.07.002

Ye, N., & Zhan, Y. (2022). Discursive identity construction of fraudsters in impersonation scam: A sociosemiotic perspective. *Journal of Zhejiang Gongshang University*, *173*(2), 17-27.

Zhou, L., Wu, J., & Zhang, D. S. (2014). Discourse cues to deception in the case of multiple receivers.

Information & Management, *51*(6), 726-737. https://doi.org/10.1016/j.im.2014.05.011

Notes

Note 1. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandAndwales/yearendingmarch2024

Note 2. https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

Note 3. https://cnnic.cn/n4/2023/0303/c88-10757.html

Note4. http://www.hydcd.com/

Note 5. https://qxk.bnu.edu.cn/#/danziDetail/49c12ccb-35cc-437b-af4a-3fe126df8fca/%E6%AC%BA/22d3af76-1ffe-46da-8c28-40e7dfe6b8d2/0

Note 6. https://cnnic.cn/n4/2024/0321/c208-10962.html

Note 7. https://m.chinanews.com/wap/detail/chs/zw/9814320.shtml

Note 8. https://weibo.com/ttarticle/p/show?id=23094045835168295160 58

Note 9. https://www.cac.gov.cn/2020-12/07/c_1608908349121859.htm

Note 10. http://www.cinic.org.cn/hy/tx/1147340.html?ivk_sa=1021577g