3L: Language, Linguistics, Literature® The Southeast Asian Journal of English Language Studies
Vol 30(4), December 2024 http://doi.org/10.17576/3L-2024-3004-04

Scheming in Syntax: Analysing Scammer-Victim Conversations in Malaysian E-Commerce Scams

NURSYAIDATUL KAMAR MD SHAH *
Academy of Language Studies
Universiti Teknologi MARA, Cawangan Melaka, Malaysia
nursyaidatul@uitm.edu.my

AMEIRUEL AZWAN AB AZIZ
Academy of Language Studies
Universiti Teknologi MARA, Cawangan Melaka, Malaysia

AMIRAH MOHD JUNED
Academy of Language Studies
Universiti Teknologi MARA, Cawangan Melaka, Malaysia

ARIFF IMRAN ANUAR YATIM
Academy of Language Studies
Universiti Teknologi MARA, Cawangan Melaka, Malaysia

WAN FARAH WANI WAN FAKHRUDDIN
Faculty of Social Sciences and Humanities
Universiti Teknologi Malaysia, Malaysia

ABSTRACT

The e-commerce scam cases reported worldwide are highly alarming, with enormous financial losses. The empirical investigation of this research focuses on the linguistic strategies utilised by scammers as their modus operandi in duping their targets. This research aims to analyse the common linguistic features of scammers and identify the steps, strategies, and patterns prevalent in e-commerce scams in Malaysia by conducting a thorough linguistic analysis of real conversation exchanges between scammers and victims. This qualitative study compiled and established a database of e-commerce scam cases from social media. From this database, 14 sets of online communications between scammers and 14 Malaysian victims were chosen and examined using the content analysis method—one facet of the data analysis involved studying scammers' linguistic styles and patterns in persuading their targets. The analysis revealed various persuasive linguistic tactics employed by the scammers to deceive the victim, which are friendly expressions, urgent disclosure, manipulated statements, persuasive language, leveraging authority declarations, fabricated social references and appealing offers. Guided by speech act theory, this study shows that scammers use locutionary acts (specific words and phrases) to appear legitimate, illocutionary acts (intentions behind the words) to make false promises or issue threats, and perlocutionary acts (impact on the victim) to evoke trust, fear, or greed. This study demonstrates how scammers use subtle yet effective language to deceive individuals out of money. Contrary to the common perception of the gullible or vulnerable person "falling for" a scam, the findings reinforce how scammers are effective language manipulators who employ strategies to reassure victims and disassemble any reason for concern. The study highlights the importance of being vigilant to these tactics and implementing caution when engaging with unfamiliar online sellers. It emphasises the need to verify sellers' legitimacy and be wary of any requests for payment before receiving the purchased item.

Keywords: content analysis; deceptive language; e-commerce scams; linguistic analysis

INTRODUCTION

Linguistics is fundamentally concerned with the nature of language and communication. People have been captivated by language and communication for thousands of years, and they have only now begun to comprehend the complexity of this aspect of human life in many ways (Akmajian et al., 2017). One of the latest topics to pique the interest of linguistic researchers is the analysis of language use on the internet and social media platforms. The Internet brings many benefits and ease to users and online consumers. The emergence of e-commerce or online shopping platforms has opened up multiple opportunities for business owners to multiply their earnings. It is also an opportunity for consumers to shop conveniently compared to traditional shopping methods. The development of the current situation opens consumers to the novel threat of fraud and scams, especially on social media and other online shopping platforms. This phenomenon is alarming as online purchases among Malaysians increase daily. A study by Zainuddin (2021) reported that in 2020, Malaysian consumers bought 50 per cent more online than in 2019, driven primarily by the COVID-19 restriction. The report further added that about 47 per cent of consumers in Malaysia switch to the online method as the most frequently used channel to make purchases of goods. It is expected that the e-commerce segment in the country has bright prospects, and it will continue to grow, supported by the population of mature adults and highly digitally literate in Malaysia, involving users aged 15 and above.

Cybercrime on various internet platforms is a growing concern and has drawn attention from authorities, policy-makers, and academicians worldwide. People with ill intent or scammers attempt to persuade others (thus known as victims) through manipulation, which can be done through language (Srour & Py, 2022). Many people might easily be cheated by the language used by scammers when influenced by scammers' manipulation language (Male et al., 2021). Victims are generally tricked by the appealing words scammers employ, even without accurate and reliable descriptions of the products and services, which can lead to poor decision-making and massive financial losses.

E-commerce scams are significant global issues, leading to enormous financial losses as scammers falsely advertise goods on e-commerce platforms and social media and disappear following receipt of payment (Hanoch & Wood, 2021; Paintal, 2021; Sinha et al., 2020; Zahari et al., 2019). The COVID-19 pandemic exacerbated this problem, particularly in Malaysia, where e-commerce scams surged during the Movement of Control Orders (MCOs). From 2018 to May 2022, Malaysia recorded approximately RM5.2 billion in financial losses due to e-commerce scams (David, 2022). The Royal Malaysia Police reported over 65,000 cybercrimes and online scams since 2017, with e-commerce being the most prevalent, followed by illegal loan and investment scams. Senior citizens, including other vulnerable groups such as students, government servants, and retirees, are frequent targets due to their perceived financial stability, social isolation, and unfamiliarity with technology (Button & Cross, 2017; Shao et al., 2019).

The COVID-19 pandemic led to a dramatic rise in reported e-commerce scam cases and financial losses from 2020 to May 2022, as lockdowns increased internet usage. Despite numerous awareness campaigns by authorities, namely, the Royal Malaysia Police (PDRM), Bank Negara Malaysia (BNM), and the Malaysian Communication and Multimedia Commission (MCMC), a large number of individuals continue to be deceived by these fraudulent schemes, with the actual figures probably surpassing what is officially reported. Research has focused on the technical aspects of scamming, such as cybersecurity, but it is equally important to examine the non-technical aspects, particularly the language scammers use. Scammers often employ convincing

language to manipulate victims through social engineering, making them believe in false promises. This manipulation involves language cues and features designed to influence and reassure victims, as noted by several studies (Male et al., 2021; McGowan, 2021; Pouryousefi & Frooman, 2019).

Scams have profound impacts that extend beyond financial losses, affecting victims' psychological well-being and leading to significant emotional and behavioural changes. Victims often experience trauma, shattered worldviews, and a loss of trust in others, as described by Whitty and Buchanan (2016). Emotional repercussions include fear, anger, suppressed emotions, and post-traumatic stress disorder, as noted by Castel (2021). The difficulty in prosecuting scammers, highlighted by M. R. A. Rahman (2020), exacerbates the issue, leaving victims in severe debt, depression, and a diminished quality of life, sometimes resulting in broken families and increased suicide rates (Sarriá et al., 2019). Despite laws such as the Financial Services Act of 2013 and various public awareness campaigns, the susceptibility of people to scams persists due to psychological manipulation (Tausczik & Pennebaker, 2010), with experts advocating for comprehensive public education as the most effective defence against scams (Kadoya et al., 2020; A. A. Rahman et al., 2020; The Sun Daily, 2022; Vayansky & Kumar, 2018).

The use of language in communication, especially on social media platforms, has made it easier for scammers to manipulate potential victims through appealing and convincing advertisements. Scammers often utilise simple yet powerful words to attract buyers on online shopping platforms, for instance, Shopee, Lazada, Facebook Marketplace, Carousel, and Mudah.com. Victims are usually unaware of the manipulation (Button & Cross, 2017; Male et al., 2021) until completed money transfer and the scammers' disappearance, leaving them with financial losses and resentment, which highlights the urgent need to identify and understand the language manipulation techniques used by scammers to prevent people from becoming victims. Relevant authorities and organisations, such as the PDRM, BNM, and MCMC, face challenges in educating the public about these scams due to the appeals of scammers' language.

Research into the linguistic strategies of authorship attribution in e-commerce scam promotional materials can reveal how scammers construct their deceptive narratives. It involves studying these materials' stylistic features and patterns to understand how they influence prospective victims' decisions. While there has been considerable research on various types of scams, including love scams, Macau scams, and Nigerian email scams, there is a lack of specific studies focusing on the authorship attribution of e-commerce scam contents, particularly in Malaysia. Therefore, comprehensive research in this area is necessary to map out the communicative patterns of scammers and provide public education on recognising and avoiding such scams. This study aims to fill that gap by analysing the linguistic features and authorship attributes of e-commerce scam narratives to enhance public awareness and prevention efforts.

LITERATURE REVIEW

Linguistic analysis of deception has garnered significant scholarly attention, aiming to understand how language can be used to mislead and manipulate. This field intersects with various disciplines, including psychology, linguistics, and communication studies, providing a comprehensive framework for identifying deceptive practices. One of the foundational theories in this field is Speech Act Theory. Speech Act Theory (Austin, 1975; Searle, 1979) can be applied to deepen the understanding of scammers' interactions and strategies when analysing conversations between scammers and victims in e-commerce scams, as it provides a framework for understanding how

language is used to perform actions. When applied to persuasive linguistic tactics, this theory provides a framework for understanding how speakers can influence others through their words. The theory identifies three types of speech acts: locutionary, illocutionary, and perlocutionary acts. Understanding how scammers use these acts can shed light on their linguistic strategies and how they manipulate their targets.

Locutionary acts involve the actual utterance and its literal meaning. In persuasion, the choice of words, clarity, and tone are crucial in ensuring the message is comprehensible and engaging. Illocutionary acts refer to the speaker's intention behind the utterance, such as asserting, requesting, promising, or expressing emotions. These acts are vital in persuasion as they reveal the speaker's purpose, whether to convince, motivate, or build rapport. Perlocutionary acts are the utterance's effects on the listener, such as persuading, inspiring, or motivating action. Effective persuasive tactics often involve a combination of emotional appeal (pathos), logical appeal (logos), and ethical appeal (ethos). Emotional appeal targets the listener's feelings, logical appeal uses evidence and reasoning to support arguments, and ethical appeal establishes the speaker's credibility and trustworthiness. By understanding and strategically employing these speech acts, speakers can craft messages that resonate with their audience's values and emotions, achieving their persuasive goals. Speech Act Theory thus provides valuable insights into the mechanics of persuasive communication, highlighting the power of language to influence and effect change.

Several studies have identified linguistic features that are commonly associated with deception. Aziz et al. (2023) analysed the linguistic cues of deception in online investment scams in Malaysia. The findings highlight the predominant use of linguistic cues in online investment scams, with the Lifestyle dimension being the most frequently used, followed by the social process, cognition, affect, and perception dimensions. The study reveals the linguistic tactics employed by scammers, such as emphasising religious sentiments, using persuasive language, and creating an illusion of sophistication to deceive potential victims. The study utilises the Linguistic Inquiry and Word Count (LIWC) software and Statistical Package for Social Science (SPSS) to analyse data from official website pages of investment scams provided by various Malaysian authorities. The correlation analysis indicates significant associations between the dimensions, suggesting that these cues are used in tandem to create convincing narratives in the scams. The study's results provide valuable insights into the linguistic patterns of deception in online investment scams, contributing to developing a possible comprehensive linguistic model for scam detection. This research is significant in the fight against online scams as it offers a preliminary exploration of linguistic cues and their correlation in online investment scams' promotional materials, potentially leading to the development of systems for automated scam detection through textual analysis.

Hua et al. (2017) investigated how hackers in China use the QQ instant messaging network to deceive users while performing fraudulent activities. Using Speech Act Theory and Politeness Theory, the study examines 50 conversations between fraudsters and their victims, demonstrating various discourse methods, including business invites, money transfers, and account hacking. Fraudsters frequently employ strong language and face-threatening speech acts to influence their victims, giving the illusion of urgency to elicit speedy replies. The study emphasises the importance of knowing the linguistic tactics scammers use to deceive users, as this can assist design models to minimise online fraud. The study recommends investigating victims' weaknesses and the reasons for their vulnerability to such deceit.

Hancock et al. (2004) looked at how the language styles of the sender and recipient varied throughout a dyadic conversation that was both honest and dishonest. A computer-based examination of 242 transcripts showed that while lying compared to speaking the truth, senders used more total words, more allusions to other people, and more sense-based descriptions (such as seeing and touching). When lied to, recipients unaware of the manipulation of deceit used more words and sense phrases, asked more questions, and used shorter sentences than when given the truth. The ramifications of these findings for linguistic style matching are examined.

An article by Nicolaides et al. (2018) examined various psycholinguistic strategies that auditors might use to analyse spoken and written language for indicators of deceit. The review is a starting point for some suggested future research topics. Keyword searches of significant bibliographic databases find relevant material from several fields. The methodologies mentioned have much potential for helping auditors find audit settings that require further in-depth inquiry. This paper compiles research on deceitful communication from several areas and connects it to the audit setting. The focus of auditors is drawn to possible language indicators of fraud risk, and possibilities for further study are proposed. The work raises awareness, has a pedagogical function, and makes necessary recommendations for a future research agenda. A common component of lying is making up a tale about an event or attitude that does not exist. False stories may, therefore, differ substantially from truthful stories.

The current effort by Newman et al. (2003) looked into the characteristics of linguistic style that set authentic stories apart from fake ones. A computer-based text analysis software correctly identified liars and truth-tellers in a study of five independent samples at a rate of 61% overall and 67% when the topic stayed constant. The findings suggest that liars had lesser cognitive complexity, utilised fewer self- and other-references, and used more terms associated with negative emotions than truth-tellers. Levitan et al. (2018) investigated how to spot lies in interview conversations. They examine several linguistic traits in both honest and dishonest interview answers. They also examine how deceit is perceived to determine whether interviewers would interpret a remark as dishonest or accurate. The data gathered reveals considerable changes in deception tendencies across gender and native language and truthful and dishonest question replies. This research guided the characteristics of machine learning studies that classified misleading speech internationally.

E-commerce has grown over the last ten years and is a significant part of our everyday lives. However, e-commerce fraud is becoming increasingly common and costs money, especially to e-consumers, who frequently do not get what they pay. Fraudsters deceive online shoppers in various ways, such as by advertising discounted items on websites to get them to make a purchase. Despite Malaysia's serious worries over e-commerce fraud, the present legal system's shortcomings mean that the legislative punishment is still insufficient. A study by Razali et al. (2022) explored the nature of e-commerce fraud, how it operates, and the legal protection Malaysian e-consumers are given. It used secondary data from scholarly publications, books, news items, internet databases, the Malaysian Penal Code, the Communication and Multimedia Act 1998, and doctrinal content analysis. The authors argued that the inadequacy of the legislation and a lack of understanding of the seriousness of such crimes are to blame for the absence of legal protection for online customers. Effective industry administration is essential to promote prosecution, investigation, and comprehensive protection for cyber fraud victims.

Prior studies have confirmed the extensive usage of social networking (SNS) platforms for online buying among social media users, sometimes referred to as social commerce. Despite the sound effects of shopping on social network platforms receiving significant attention in the

literature, the negative implications of this commerce have not been well studied. Notably, the frequency of cybercrime, particularly fraud involving online purchases, has grown. Talib and Rusly (2020) examined online buying fraud incidents involving purchases made through social network platforms, the demographics of the victims, and the economic effect of the fraud on the victims to close this gap. Additionally, the paper also looked at fraud case mitigation techniques. An online poll was used to collect information from users of social networks. According to the results, Facebook is the most widely used social network site for shopping, with about 70% of the respondents now doing so. Up to 24 per cent of persons who engage in social commerce acknowledged having fallen victim to purchasing fraud. Most victims were married, highly educated women between the ages of 26 and 35 with middle-class incomes. Most of the victims suffered cash losses totalling close to RM400. Some mitigating techniques include word-of-mouth, background checks on sellers, dependable and transparent transaction processes, and avoidance.

Scammers use a variety of con tricks to cheat their victims. One of the most typical methods is to use mules to help them (M. R. A. Rahman, 2020). The pertinent Malaysian legal regulations that are used to stop these criminal actions are discussed in this article. The goals are to draw attention to the importance of sections 415 and 420 in dealing with online fraudsters and sections 414 and 424 in dealing with mule participants. Pertinent examples are also referenced to help readers comprehend the situation surrounding these con artists and their mules. From the studies mentioned, understanding scammers' linguistic and psychological manipulation strategies is crucial for developing effective prevention, detection, and legal measures to combat e-commerce scams.

METHOD

This study aims to analyse the common linguistic traits of scammers and uncover the steps, strategies, and patterns common in Malaysian e-commerce scams by performing a detailed linguistic analysis of actual conversation exchanges between scammers and victims. This study employed the qualitative approach to content analysis. The data of this study was analysed based on Zhang and Wildemuth's (2017) qualitative content analysis method as it is a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns. The sample for this study is taken from social media postings by the alleged scam victims. Social media platforms, such as Facebook, produce large amounts of data, making them suitable for data collection platforms due to their volume, velocity, and dynamism (Alzahrani, 2016). This study employed purposive sampling to align the samples with the research aims and objectives. The sampling process was done by seeking potential scam victims that meet the study's requirements.

This study analysed the conversations between victims and scammers on Facebook posts. Data was collected from relevant screenshots from scam victims' postings on Facebook related to the *Emas Lelong* or 'Gold Auction' transaction. The researchers also looked for screenshots shared by the scam's victim shown on the 'explore' page using keywords such as *scam emas lelong* or 'gold auction scam'. The researchers then determined whether the posts were suitable to be used as data for the research. The document depicts a series of messages between a scam victim and a scammer attempting to deceive the victim into making multiple payments under pretences. The scammer claims to facilitate an official auction act for the victim's name and requests payments

for various reasons, such as a signature replacement guarantee, gold redemption certificate, and auction letter. The scammer assures the victim that the money will be returned within a short timeframe, often 5-15 minutes, and employs persuasive language, urging the victim to borrow money and assuring that the payments are necessary and will be fully refunded. The victim expresses distress, frustration, and scepticism throughout the conversation as they realise they are being scammed. The scammer also attempts to entice the victim with offers of free gold items and bonus incentives for making payments. Additionally, the scammer insists on immediate payment, using the excuse of potential legal consequences or complications with the delivery of purchased items to pressure the victim into complying.

In qualitative research, the data collection reaches a saturation point when the data collection ceases to add value. In this study, data saturation occurs when further data collection fails to reveal new themes, patterns, or information, indicating that the data set is comprehensive and adequately captures the phenomenon under study (Saunders et al., 2017). The postings by scam victims were collected and sorted. These screenshots of conversations were then transcribed and coded for further analysis following Zhang and Wildemuth's (2017) qualitative content analysis procedures. The code, category, and theme for each posting were then determined. After coding, it was then put into a thematic diagram to understand the themes better.

RESULTS

The data analysis of real conversation exchanges between scammers and victims in e-commerce scams in Malaysia manages to identify an emerging pattern in linguistic features used by the scammers, as illustrated in FIGURE 1.

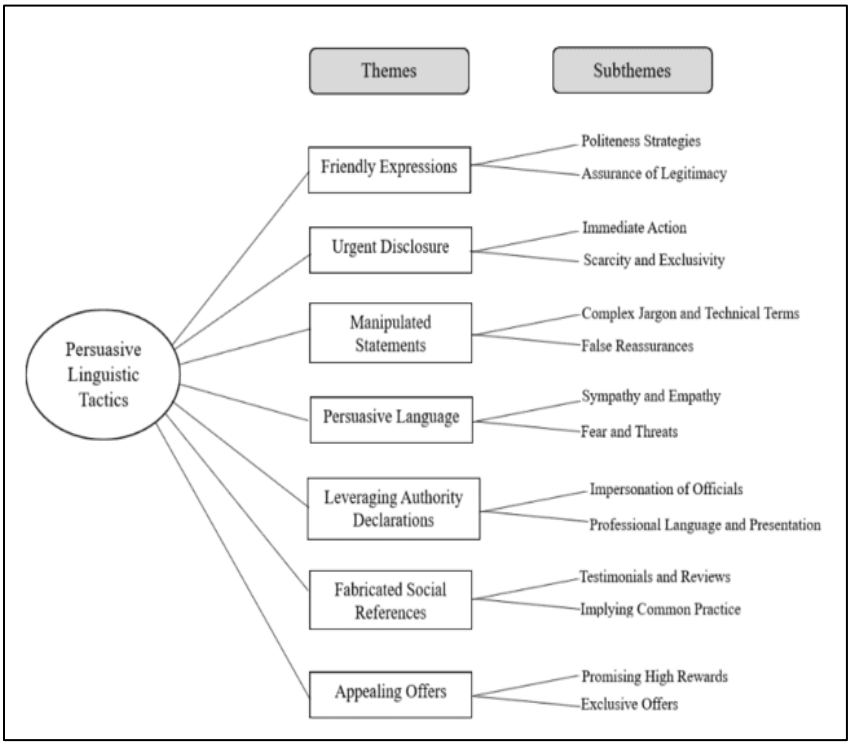

FIGURE 1. Patterns of Linguistic Tactics Used by Scammers

Through speech act theory, the analysis of conversations between victims and scammers on Facebook pages reveals how scammers strategically use language to deceive and manipulate their targets. The locutionary acts involve the specific words and phrases used, crafted to appear legitimate and trustworthy, often mimicking the style of reputable organisations. The illocutionary acts highlight the intentions behind these words, such as making false promises, issuing urgent commands, or delivering threats to prompt immediate action. Perlocutionary acts focus on the emotional impact on the victims, aiming to evoke fear, urgency, trust, or greed to influence their decisions. Table 1 illustrates the thematic analysis of persuasive linguistic tactics identified and used by the scammer in the conversation according to the speech act.

TABLE 1. Thematic Persuasive Linguistic Tactics by Speech Act

Speech Act	Theme	Subtheme/Category	Example/Coding
Locutionary	Friendly expressions	Politeness Strategies	"Sis", "please," and "Thank you."
		Assurances of Legitimacy	"guarantee", "official," and "certificate"
	Urgent Disclosure	Immediate Action	"Immediately", "now," and "today."
		Scarcity and Exclusivity	"limited time offer" and "only a few items left."
Illocutionary	Leveraging authority declarations	Impersonation of Officials	“my boss is waiting." “Lelong Committee”
		Professional Language and Presentation	“This Lelong Gold Redemption Certificate is used to ensure the safety of the gold items until they reach the customer.”
	Fabricated social references	Testimonials and Reviews	"Many customers have already benefited from this offer."
		Implying Common Practice	"Most people complete the payment within 24 hours."
	Manipulated Statements	Complex Jargon and Technical Terms	“You need to make a deposit of RM1500 to release the ‘Official Auction Act’ in your name as the buyer and auction winner.” “This Lelong Gold Redemption Certificate is used to ensure the safety of the gold items until they reach the customer.”
		False Reassurances	"you can trust me." "This is a secure transaction."
Perlocutionary	Persuasive Language	Sympathy and Empathy	“Please try to make an effort, sis.” “Astaghfirullah, sis, I never intended to do that.”
		Fear and Threats	“It only takes 5-10 minutes. If you don't have this letter, you'll have to deal with the police and an RM35,000 fine because there's no official document from the original owner.” “Because if there is no official letter, you'll have to deal with the police station and a fine of RM5000, as there won't be an official letter from the original owner.”
	Appealing Offers	Promising High Rewards	“For ordering two gold items, we're offering one free 20g gold item."
		Exclusive Offers	“For future orders, you won't need to pay for the letter because you'll be a member”.

LOCUTIONARY SPEECH ACT

The locutionary acts are the specific words and phrases used to appear legitimate and trustworthy, frequently imitating the style of reputable organisations. Scammers frequently use friendly expressions as politeness strategies to create a friendly and trustworthy persona. The use of terms

like "sis," "please," and "thank you" is indicative of positive politeness tactics aimed at making the victim feel comfortable and respected. This approach reduces suspicion and encourages the victim to engage more openly with the scammer. Addressing the victim as "sis" creates a sense of familiarity and solidarity, making the interaction seem more personal and less transactional. Meanwhile, scammers often provide assurances of legitimacy through phrases like "guarantee," "official," and "certificate." These terms are intended to convince the victim of the transaction's authenticity or offer, countering any doubts they might have. Mentioning an "official certificate" or "guaranteed delivery" can make the victim feel that the scammer is a credible and reliable entity. Next, scammers use time-related words like "immediately," "now," and "today" to create a sense of urgency of immediate action. This tactic pressures the victim to act quickly, reducing their time to think critically or seek advice. Urging the victim to "transfer the money immediately" to secure a deal or avoid penalties creates a sense of emergency, prompting hasty decision-making. Scammers also make sense of scarcity and exclusivity by implying that the offer is limited in quantity or time, enhancing the perceived value and urgency of the transaction. Words like "limited time offer" or "only a few items left" can trigger a fear of missing out (FOMO). Claiming that "only a few units are left" and that they will be gone "by the end of the day" compels the victim to act swiftly to avoid losing out.

ILLOCUTIONARY SPEECH ACT

Illocutionary acts emphasise the objectives behind the words, such as making false promises, issuing urgent directions, or delivering threats to compel immediate action. Scammers are believed to impersonate authority figures or entities, such as 'boss' or 'committee', to enhance their credibility, which includes pretending to be from banks, government agencies, or well-known companies. By leveraging the perceived authority of these entities, scammers can more easily convince victims to follow their instructions. A scammer claims to be a bank official and uses formal language and banking terms to reinforce their authority. Phrases such as 'my boss is waiting' and 'Lelong Committee' make the victim more likely to comply with their demands. At the same time, using professional and formal language helps scammers project an image of legitimacy and seriousness. For example, the phrase 'This Lelong Gold Redemption Certificate is used to ensure the safety of the gold items until they reach the customer'. This tactic uses proper grammar, technical terminology, and a structured communication format to mimic legitimate business correspondence. Next, scammers appear to fabricate testimonials or reviews to create the illusion that others have successfully engaged with them using social references. Statements like, "Many customers have already benefited from this offer," serve as a social proof tactic that leverages the psychological tendency to follow the behaviour of others, especially in uncertain situations. Fake reviews or testimonials praising the scammer's services or products can make the victim feel more confident about proceeding with the transaction. By suggesting that many others have taken similar actions, scammers can pressure the victim to conform, which can be particularly effective if the victim believes they are part of a larger, normalised process. Statements like "Most people complete the payment within 24 hours" can push the victim to act quickly to align with perceived social norms. Furthermore, based on the conversation, the scammer tends to manipulate the victims with statements using complex jargon or technical terms that can make scammers appear knowledgeable and authoritative. This tactic helps create a perception of expertise, persuading victims to comply with requests. Referring to specific banking procedures or financial terms that the victim may not fully understand can make the scammer seem more legitimate and

authoritative. In addition, scammers provide false reassurances to alleviate any doubts or concerns the victim may express. Statements like "You can trust me" or "This is a secure transaction" are designed to ease the victim's apprehensions. If a victim hesitates, the scammer uses phrases such as “I assure you, this is completely safe and secure” to reinforce a sense of trust.

PERLOCUTIONARY SPEECH ACT

Perlocutionary acts focus on the emotional impact on the victims, attempting to elicit fear, urgency, trust, or greed to influence their decisions. Scammers might share personal or religious stories, appealing to the victims’ empathy and emotions and luring the victims to help or cooperate. From the conversation, phrases such as "Please try to make an effort, sis" and "Astaghfirullah, sis, I never intended to do that" demonstrate attempts by the scammer to appear sympathetic and empathetic towards the victim, simultaneously manipulating them into making payments. Conversely, scammers can also use fear and threats to coerce victims into compliance, which might involve threats of legal action, penalties, or other negative consequences if victims do not comply. Threatening (“If you don't have this letter, you'll have to deal with the police and an RM35,000 fine” and “because if there is no official letter, you'll have to deal with the police station and a fine of RM5000”) can intimidate victims and push them to comply out of fear of repercussions. At the same time, scammers frequently promise appealing offers such as high rewards or returns to entice victims. This appeal to greed can cloud victims’ judgments, making them more likely to take risks they usually avoid. Offering significantly discounted prices, bonus products, or unrealistic returns on investment can lure victims into believing that fantastic deals have been sealed. From the data collected, victims were offered one free item with every two items purchased by claiming, “For ordering two gold items, we're offering one free 20g gold item.” Other than that, phrases such as “For future orders, you won't need to pay for the letter because you'll be a member” present offers as exclusive because limited-time deals can make them appear more attractive. This tactic leverages the scarcity principle, where people perceive higher value in things that are rare or available for a limited time. Claiming that the offer is only available to a select few or for a limited period can create a sense of urgency and desirability.

FURTHER DISCUSSIONS

This study offers valuable insights into the linguistic strategies used in e-commerce scams, but several limitations exist. First, the small sample size of 14 conversation sets may not capture the full diversity of scams across various platforms, regions, or scam types, limiting the generalisability of the findings. The focus on Malaysian e-commerce scams also restricts the study's applicability to other cultural contexts where scamming techniques and language use may vary. The reliance on content analysis of text-based interactions also excludes other communication modes, such as voices or videos, which may involve different linguistic or non-verbal cues. Furthermore, the study primarily examines the scammers’ language without delving deeply into the victims’ responses or vulnerabilities, which could provide a more comprehensive understanding of why specific individuals fall for scams. Finally, publicly available social media posts introduce potential bias, as more extreme or unusual cases are likely to be shared, possibly skewing the data toward specific scam techniques or victim profiles.

Future research might better address the limitations of this study by expanding the dataset to include a wider variety of scam types, regions, and communication platforms, allowing for more generalisable findings. Incorporating other forms of communication, such as phone calls or video chats, might provide a more comprehensive view of scamming strategies that extend beyond text-based interactions. Additionally, exploring the psychological and social factors that make individuals more vulnerable to scams would offer deeper insights into victim behaviours and decision-making processes, enabling the development of more targeted prevention strategies. Future research can advance our understanding of e-commerce scams and contribute to more effective prevention measures by addressing these areas.

CONCLUSION

This study illustrates the growing threat of e-commerce scams and their severe financial and emotional consequences, aggravated by the COVID-19 pandemic. On the one hand, victims frequently face substantial psychological pain, such as fear and depression; on the other hand, the pursuit of scammers is a daunting task, causing financial devastation for many. The study analyses 14 online communications between scammers and Malaysian victims to identify key linguistic strategies such as friendly language, a sense of urgency, manipulated statements, authority exploitation and fabricated social proof, all intended to build trust and emotionally manipulate victims. Understanding these strategies can aid in developing educational resources and detection systems, protecting potential victims by raising public awareness, promoting critical thinking, and verifying seller validity before purchases. This study emphasises the role of linguistic analysis in preventing e-commerce fraud and calls for increased public awareness of deceptive activities in the digital marketplace.

ACKNOWLEDGEMENTS

This research was supported by the Ministry of Higher Education and Universiti Teknologi MARA through the Fundamental Research Grant Scheme (Grant No. FRGS/1/2022/SSI0/UITM/02/10).

REFERENCES

Akmajian, A., Farmer, A. K., Bickmore, L., Demers, R. A., & Harnish, R. M. (2017). *Linguistics: An introduction to language and communication*, MIT Press.

Alzahrani, H. (2016). Social media analytics using data mining. *Global Journal of Computer Science and Technology*, *16*(4), 9-16.

Austin, J. L. (1975). How to do things with words: *The William James lectures delivered at Harvard University in 1955*. Oxford University Press.

Aziz, A. A. A., Sharif, N. A. M., Fakhruddin, W. F. W. W., Juned, A. M., Shah, N. K. M.,
Yatim, A. I. A., & Saidalvi, A. (2023). Linguistic cues of deception in Malaysian online investment scams' promotional materials. *GEMA Online Journal of Language Studies*, *23*(4),152-168.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.

Castel, A. D. (2021, April 14). Fool me once: Why scams leave people feeling foolish. *Psychology Today*. Retrieved September 10, 2022, from https://www.psychologytoday.com/us/blog/metacognition-and-themind/202104/foolme-once-why-scams-leave-people-feeling-foolish

David, A. (2022, August 4). RM5.2b in losses through online scams since 2020. *New Straits Times*. Retrieved September 10, 2022, from https://www.nst.com.my/news/crime-courts/2022/08/819331/rm52b-losses-throughonline-scams-2020

Hancock, J. T., Curry, L. E., Goorha, S., & Woodworth, M. T. (2004). Lies in conversation: An examination of deception using automated linguistic analysis. *Proceedings of the Annual Meeting of the Cognitive Science Society*, *26*(26), 535–540.

Hanoch, Y., & Wood, S. (2021). The scams among us: Who falls prey and why. *Current Directions in Psychological Science*, *30*(3), 260-266.

Hua, T. K., Abdollahi-Guilani, M., & Zi, C. C. (2017). Linguistic deception of Chinese cyber fraudsters. *3L: Southeast Asian Journal of English Language Studies*, *23*(4), 108-122.

Kadoya, Y., Khan, M. S. R., & Yamane, T. (2020). The rising phenomenon of financial scams: Evidence from Japan. *Journal of Financial Crime*, *27*(2), 387-396.

Levitan, S. I., Maredia, A., & Hirschberg, J. (2018). Linguistic cues to deception and perceived deception in interview dialogues. *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT)*, 1941–1950. https://doi.org/10.18653/v1/N18-1176

Male, H., Murniarti, E., Gunawan, R., & Simatupang, M. (2021). Linguistic manipulation by
scammer as cyber crime: Viewed from law and education. *Proceedings of the 1st International Conference on Law and Human Rights (ICLHR)*, 342-350. https://doi.org/10.4108/eai.14-4-2021.2312842

McGowan, E. (2021, July 29). How to identify the language tech support scammers use to scam. *Avast Blog*. Retrieved September 10, 2022, from https://blog.avast.com/techsupport-scammer-language-avast

Newman, M. L., Pennebaker, J. W., Berry, D. S., & Richards, J. M. (2003). Lying words: Predicting deception from linguistic styles. *Personality and Psychology Bulletin*, *29*(5), 665–675. https://doi.org/10.1177/0146167203251529

Nicolaides, R., Trafford, R., & Craig, R. (2018). Helping auditors identify deception through psycholinguistics. *Journal of Financial Crime*, *25*(4), 1062–1076. https://doi.org/10.1108/JFC-05-2017-0042

Paintal, S. (2021). E-commerce and online security. *International Journal of Management (IJM). 12*(1). 682-687.

Pouryousefi, S., & Frooman, J. (2019). The consumer scam: An agency-theoretic approach. *Journal of Business Ethics*, *154*(1), 1-12.

Rahman, A. A., Azmi, R., & Yusof, R. M. (2020). Get-rich-quick scheme: Malaysian current legal development. *Journal of Financial Crime*, *28*(1), 49-59.

Rahman, M. R. A. (2020). Online scammers and their mules in Malaysia. *Jurnal Undang-Undang Dan Masyarakat*, *26*, 65–72.

Razali, N. A. H., Wan Rosli, W. R., & Othman, M. B. (2022). The legal protection of e-consumers against e-commerce fraud in Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *7*(9), 1-9. https://doi.org/10.47405/mjssh.v7i9.1778

Sarriá, E., Recio, P., Rico, A., Díaz-Olalla, M., Sanz-Barbero, B., Ayala, A., & Zunzunegui, M.
V. (2019). Financial fraud, mental health, and quality of life: A study on the population of the city of Madrid, Spain. *International Journal of Environmental Research and Public Health*, *16*(18). 3276. https://doi.org/10.3390/ijerph16183276

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2017). Saturation in qualitative research: Exploring its conceptualisation and operationalisation. *Quality & Quantity*, *52*, 1893 - 1907. https://doi.org/10.1007/s11135-017-0574-8

Searle, J. R. (1979). *Expression and meaning: Studies in the theory of speech acts*. Cambridge University Press.

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse and Neglect*, *31*(3), 225–243. https://doi.org/10.1080/08946566.2019.1625842

Sinha, P., Sharma, U., Kumar, D., & Rana, A. (2020). A Conceptual framework for mitigating the risk in e-commerce websites. *Proceedings of the 8th International Conference on Reliability, Infocom Technologies and Optimisation (Trends and Future Directions) (ICRITO)*. 217-221.

Srour, C., & Py, J. (2022). The general theory of deception: A disruptive theory of lie production, prevention, and detection. *Psychological Review*, *130*(5), 1289-1309.

The Sun Daily. (2022). *Empowering the public against online harm.* https://www.thesundaily.my/spotlight/empowering-the-public-against-online-harm-FM9592887

Talib, Y. Y. A., & Rusly, F. H. (2020). The current state of social commerce fraud in Malaysia and the mitigation strategies. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(2), 1593–1599. https://doi.org/10.30534/ijatcse/2020/105922020

Tausczik, Y. R., & Pennebaker, J. W. (2010). The psychological meaning of words: LIWC and computerised text analysis methods. *Journal of Language and Social Psychology*, *29*(1), 24–54. https://doi.org/10.1177/0261927X09351676

Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security, 2018*(1), 15-20.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.

Zahari, A. I., Bilu, R., & Said, J. (2019). The role of familiarity, trust and awareness towards online fraud. *Journal of Research and Opinion*, *6*(9), 2470-2480.

Zainuddin, M. Z. (2021, October 19). Separuh rakyat Malaysia beli barang dalam talian. *Berita Harian*. https://www.bharian.com.my/bisnes/lain-lain/2021/10/877743/separuh-rakyat-malaysia-beli-barang-dalam-talian

Zhang, Y., & Wildemuth, B. M. (2017). Qualitative analysis of content. *Applications of Social Research Methods to Questions in Information and Library Science*, 318-329. Santa Barbara, CA: Libraries Unlimited.