3L: The Southeast Asian Journal of English Language Studies – Vol 23(3): 108 – 122
http://doi.org/10.17576/3L-2017-2303-08

Linguistic Deception of Chinese Cyber Fraudsters

TAN KIM HUA
Sustainability of Language Sciences Research Centre,
Faculty of Social Sciences and Humanities,
Universiti Kebangsaan Malaysia

MOHAMMAD ABDOLLAHI-GUILANI
Buein Zahra Technical University,
Buein Zahra, Qazvin, Iran
abdollahi20@gmail.com

CHEN CHEN ZI
Independent Scholar, Xi'an,
Shaanxi Province, China

ABSTRACT

Cybercrimes are on the increase in China and 'QQ', an instant messenger platform, is frequently exploited for these crimes. Fraudsters manipulate language to deceive users into revealing their bank accounts or depositing sums in the cheats' accounts. Employing the theoretical framework that includes Speech Act Theory and Politeness Theory, the researchers attempted to identify the strategies used by such fraudsters. The subjects of this study included 50 interlocutors who had already chatted with different online cheats and had a record of their conversations. The data were collected and analysed on the basis of the type of discourse themes displayed. Findings indicated that the chats displayed various themes like Business Invitation, Money Transfer, Account Hacking and Online Shopping. In addition, the three levels of speech acts of locutionary, illocutionary, and perlocutionary were discernible and most fraudsters did not bother to address face threatening acts. In comparison to hoax email writers, the fraudsters in instant communication regularly came across as more aggressive and imperative, but then softened their diction if victims were not interested to chat with them in real time. The implications of this study lie in the possibility of developing a model for fraudster or cheat discourse structure, thus alerting QQ users in particular of such crimes. Other online instant messenger users will also benefit from this study. Better informed of how cheats manipulate language to present untruth as truth and be alerted of the modus operandi involved in online deception, victims can be saved and the crime curbed. The issue of the victim's vulnerability and the reasons behind it certainly deserve further linguistic and metalinguistic scrutiny.

Keywords: cybercrimes; fraudsters; linguistic deception; speech acts; politeness

INTRODUCTION

People are reportedly said to be telling one to two lies per day on average. Therefore, deception is not an infrequent part of human communication. Additionally, research shows that lies also take place in computer-mediated communication (Hancock et al. 2008). With the development of the Internet, the network seems to become a new kind of crime tool, crime place and crime object (Guo 2011). Due to the increasing usability of the Internet, most communicators can remain anonymous and this has created new opportunities for deception and scams (Hancock 2007, Blommaert 2005).

Statistics showed that in 2007 the number of Internet users in China exceeded 162 million and 69.8% of them (over 113 million users) used Instant Messengers (IM) such as QQ, MSN Messenger, and Yahoo Messenger. Among these social networking platforms, QQ, developed by the Chinese company Tencent, currently occupies about 80.1% of the IM market share in China (CNNIC 2007, cited in Lu, Zhou & Wang 2009).

The popularity of QQ brings benefits not only to the Information Technology market, but also to the treacherous fraudsters or cheats around the Internet space. They manipulate this platform and figure out ways to make easy profits. Guo (2011), analysing the cases and summarising the main forms of Internet frauds, stated that in China, one of the most frequent cybercrimes is QQ hacking frauds. A lot of users claimed they fell into the "QQ-friends-borrow-money" trap, and lent money to the so-called friends or relatives. This is the kind of fraud after QQ accounts were stolen. The cheats hacked someone's QQ account, then impersonated as a relative or a known friend and successfully borrowed money. As QQ is an online chatting tool, the whole cheating process was done through conversation. Such cybercrime can also be seen as language crime, because it is executed via texts, and thus aptly studied from a linguistic perspective.

With the anonymity provided by the Internet, users undertake false identities to engage in deceptive communication. Detecting deception is thus, difficult. Although electronic dictionaries have the technical ability of linking to an application and providing a platform for detecting the common terms used by fraudsters, as stated by Tan and Woods (2008), lexical items detection is rendered less useful unless the architecture of the whole cheat scheme is unravelled. It is, therefore, imperative to be aware of the linguistic architecture used and the intentions of fraudsters.

As this study unravels the relationships between linguistic forms and the language users of these forms, people's intended meanings, assumptions, and goals, as well as identifying the kinds of actions that they are performing while chatting are detected (Yule 1998). Careful investigation is required to uncover the cheats' devious intentions. It is essential to find out what kind of words cheats use when they attempt to deceive victims, and why the victims fall prey to cheats. More importantly, even if it were the victims' friends or relatives who asked to borrow money, it is important to find out how the cheats could achieve the goal effortlessly.

This study analysed the module of cheats' language in deception by examining the following:

1. The discourse structure of the QQ hacking frauds in the data
2. Pragmatic strategies in the openings and closings of cheats' speech as in greeting and politeness strategy.
3. The way cheats perform speech acts at every phase of cheating within the conversation.

In order to accomplish the above-mentioned objectives, the following research questions are brought into concern:

1. What types of discourse structures were applied in the data of QQ hacking frauds?
2. How did the cheats apply pragmatic strategies in the openings and closings?
3. How did the cheats perform speech acts at every phase of cheating within the conversation?

LITERATURE REVIEW

Of all human behaviours that are considered to breach conventions of social and communicative interaction, deception is one of the most pervasive and by far the most elusive (McCarthy, Duran, and Booker 2012). Deception is part of daily personal as well as business life and usually involves messages that are delivered in order to mislead others or to persuade

others to believe what is said, even if it is not true (Zhou et al. 2003, Hancock et al. 2004 cited in Galanxhi & Nah 2007).

The concept of deception is mundanely known as lie, cheat, or bluff. Xie and Lin (2005, as cited by Yao bin Lu et al. 2009) stated that lies are always defined as declarations that are intended to let others misunderstand, and to expect others to believe what is said; it is a violation of what is known to be true for the purpose of misleading, but seemingly trustworthy information (Ekman 1997, cited in McCarthy, Duran & Booker 2012). In this respect, Coleman and Kay (1981) argue that there are levels within lies; the action of lying is the surface of deceptive intention, and needs to fulfil three factors:

a) the sender knows the statement is untrue,
b) the sender intends to cheat the receiver
c) the untruth of the sender's declaration can be proven.

The identity of the cheats largely affects victims' level of acceptance; it is the first factor the cheats manipulate, because they are portraying the person that shares some relationship with the victims.

According to Ekaning (2011), crimes that are formed through language can be studied from a different viewpoint. Language can form insult, threat, fraud, perjury, forged and fake advertisements, and plagiarism. Even crimes like theft, kidnapping and murder, which require language before realization, can be considered as language crimes. Through different cases such as e-mail scams and Instant Messenger traps, researchers explore how deception affects language use in text-based interactions in order to identify linguistic patterns and differentiate between deceptive and truthful electronic communication (Hancock et al. 2008).

Zhou et al. (2002) mentioned two conceptions that reveal weaknesses in deception. One is language complexity while the other is language diversity. As a complex task, deception requires more cognitive processing than telling the truth. Faced with such cognitive challenges, deceivers have to monitor any suspicion aroused on the receiver's side while communicating with them. However, it is likely that the cheats produce messages with lower language complexity for the complex task than truth-tellers do. The second feature, language diversity too, can probably betray cheats. The language used for describing fake events may fail to reflect the rich diversity of actual events because cheats usually lack truthful memory or experience. Literature suggests that cheats often display less diversity at both lexical and content levels (Zhou et al. 2002).

Most researches focus on email hoaxes rather than conversational text-based frauds. The computer-mediated discourse of the conversation, which is produced when people interact with one another via networked computers, is text-based; messages are typed on a computer keyboard and read as text on a computer screen, typically by people at different locations (Herring, Stein & Virtanen 2013). Chiluwa (2009, 2010) stated that there is an increasing application of Internet resources especially emails in digital deceptions particularly financial scams. All forms of frauds on the Internet begin from the point of using language in a particular way, to persuade and eventually convince others. In the email hoax cases, all of Searle's (1979) five categories of speech acts were performed in written texts. His analyses showed how the various communicative or persuasive strategies in the emails actually employed most or all of the speech acts such as requesting, greeting, and commanding. Studies (e.g., Blommaert 2005, Chiluwa 2010) on spam emails from a linguistic perspective revealed that the English proficiency of the writers of the deceptive email however, do not match their level of digital literacy. They displayed expertise in detecting victims but failed in some text structures such as normative codes of their addressees which resulted in misnomers.

THEORETICAL FRAMEWORK

The theory of discourse analysis applied here is one of strategy that views discourse as a social practice (Fairclough 1989). Computer-mediated communication in this context is such that all forms of communication or messages produced and transmitted through computer networks are viewed as discourses, revealing features of real life identities and dimensions of social practices. Because it focuses on language and language use in computer network environments, computer-mediated discourse analysis examines language use and how the different linguistic properties are influenced by their socio-cultural context. According to Herring (2001), computer-mediated discourse analysis will pay attention to how users of the networks do interactional work through text-based discourses, allowing them to negotiate, intimidate, joke and of course cheat and deceive.

Based on the property of the emails, Chiluwa (2010) identified and classified cheat's intentions into themes namely (i) money transfers, (ii) next-of-kin claims, (iii) fortune bequeathing, (iv) charity donations and (v) investment opportunity. The module of deception, following Chiluwa (2010) has the below discourse structure:

1. Opening/greeting
2. Introduction (including the identity of the writer and often an apology for making contact without prior notice)
3. A narrative which includes a description of:
   (i) the origin of the money deposited in a foreign account in which the addressee is made a beneficiary;
   (ii) a painful experience of the death of a spouse and the money he kept in a dormant account abroad to be used for charity or for raising his kids;
   (iii) a story of a wealthy client who deposited some millions of dollars in a foreign account and had died, leaving the money for the addressee; or
   (iv) an investment opportunity abroad worth millions of dollars
4. An invitation to the receiver to be engaged in the business with an offer of a profit-sharing formula
5. Request for confidentiality or an invitation to the addressee to indicate interest
6. Closing (pressing a request to the receiver to reply immediately)

In addition to Chiluwa's perspective, the speech act theory (Searle, 1979) and politeness theory supported and formed the framework of this study.

METHODOLOGY

This study applied both a qualitative and quantitative research method to explore how people utilised language to achieve their goals. The content-based analysis approach is functional in decoding language used in the cheat's discourse. According to Robichaud and Blevins (2011), the most fundamental form of content-based text analysis is that of counting words. In addition, content analysis allows the researcher to test theoretical issues to enhance understanding of the data (Satu & Helvi 2007). There are various elements in written messages that can be counted, such as words, themes, and items. In this study, several themes within the cheats' speech were counted such as the way the interlocutors greeted and how often certain phrases appeared in a text. Concepts behind the cheats' speech were also quantified, such as the speech acts they performed. Two theories, namely politeness strategy

and speech acts taxonomy, were used to analyse the data. Aspects of these theories decode what people have in mind when they use language for socialization.

RESEARCH SAMPLE

In this study, the participants were cyber interlocutors including those who were considered the victims of lies and cheats pretending to be the victims' friends. In the researchers' QQ friend list, there were 343 people. About 70% of them were the researchers' relatives and the rest were just online friends whom the researchers did not know personally. Since not everyone had the experience of chatting with cheats, the researchers approached friends individually, and published announcements through QQ inquiring if anyone indeed had the experience of chatting with cheats and had records of the conversation. This was voluntary. During the consultation process, half of the QQ friends stated they did not save chatting records, and most of them had not chatted with cheats. However, from April 2016 to September 2016, 50 pieces of relevant conversation data were collected; this led to 50 victims and 50 cheats who contributed to the chatting records forming the corpus of the present study. Because all of the QQ hacking frauds happened in China, all the cheats were Chinese QQ software users, but their locations and genders were unknown.

DATA COLLECTION METHOD

When the researchers' QQ friends agreed to contribute, they emailed the researchers a copy of their chatting records. Subsequently, the texts that the cheats and the victims typed out were translated from Chinese into English. The duration of each conversation ranged from 1 minute to 10 minutes or more. Some of the conversations were monologues and contained only one turn, while some dialogues could reach up to tens of turns.

RESULTS

According to the features of the conversations, four types of frauds were examined as given in Table 1.

TABLE 1. Types of conversation

BI	SO	MT	AH	Total
7	7	29	7	50

Table 1 indicates that there are four types of conversation, namely business invitation (BI), help to do shopping online (SO), money transfer (MT), including money borrowing, money changing, and money keeping, and QQ account hacking (AH). The table shows that the highest frequency of conversation revolved around the subject of asking victims to transfer money to a certain account, but the other types each had 7 instances of occurrences.

The first type which was business invitation often appeared as a poem-like monologue. The texts always started with some idioms or sayings to create a convincing and unforced atmosphere, and then developed into invitation to readers to join a chatting group or to add some QQ accounts as QQ friends. The context usually revolves around some quick ways of earning money, or developing chatting groups for making money.

In the second type, shopping online, the cheats usually pretended to be the victims' friends and requested for online shopping and then promised that once the transaction was done, they would return the money to the victims.

Money transfer was the third type of the cheats' conversation. Here the cheats pretended to be the person whose QQ account was stolen, and requested the victims to deposit or transfer money to the cheats' friends. This category was further subdivided into three types: Money Borrowing, Money Changing, and Money Keeping.

In the Money Borrowing case, the cheats claimed the victims' friends were in dire need of help and they asked the victims to lend them some money so that they could transfer that sum to their mutual friends' accounts. The cheats offered a bank account which was either their own account or belonged to one of their accomplices.

In the Money Changing case, the victims were overseas students' parents or relatives. The cheats pretended to be those students and claimed that their classmates or friends around wanted to exchange currency with them. Some of the cheats also claimed that their friends had trouble in China, and hence urged the victims to transfer money to their friend's relatives in China immediately. In these cases, the cheats assured they would return the money, too.

In the Money Keeping cases, instead of borrowing or asking for money from the victims, the cheats claimed that they lost their personal bank card, so they wanted to transfer their money to the victims' bank account. Meanwhile, they asked for the victims' identity card number and bank card bound phone number. In such cases, the cheats would utilize the information they asked from the victims to open an online bank account. After that, the cheats would say that they had already made the deposit, and asked for a code to check whether the money was safe. Once the victims gave the cheats the code, all the money in the victims' bank account would be taken by the cheats.

The fourth type was account hacking. Here the victims were required to lend the cheats QQ accounts and passwords so that the cheats could test certain applications or play online games. Once the victims gave the cheats their passwords, the cheats would change the passwords immediately. Another way was that the cheats would request the victims to 'help to vote for a friend in a competition' by logging in to a website with the victims' QQ accounts, and as soon as the victims logged in to the website, their passwords would be hacked by the cheats.

Consulting the research contributors, the researchers managed to learn how many cheating attempts were successful as given in Table 2 below:

TABLE 2. Successful and failed frauds

	Data	Frequency	Rate%
Successful frauds	AH1-2, AH7, MT14-15, MT24-25, MT28-29, SO1-2	11	25.6
Failed frauds	AH3-6, MT1-13, MT16-23, MT 26-27, SO3-7	32	74.4
	Total	43	

Table 2 shows that except for business investment whose exact number of successful and failed fraud attempts could not be confirmed by the research contributors, the other cases indicated that the number of failures were almost three times higher than that of the successes (32 vs 11). In the table, the numbers appearing after the acronyms show the research subjects ID who were randomly listed. It shows that the successful cases in account hacking, money transfer and online shopping were 3, 6, and 2, respectively, while the results for the failed attempts included 4, 23, and 5 cases, respectively.

ANALYSIS OF CHEATS' TEXTS and DISCUSSION

The collection of the cheats' conversations with the cyber victims provided an opportunity to analyse the data in terms of forms and structures. The cheats' behaviour showed that they would make up a story and ask for money, fix their lies when the victims suspected, and

eventually convinced victims into doing what they were asked to. Since the cheats were pretending to be the victims' friends, they casually chatted with the victims, and so most of the conversations were structured as (i) opening, (ii) chatting, and (iii) closing. However, most of the conversations did not get a clear close at the end, because either the cheats were discovered by the victims at this stage or they urged the victims to take action.

As for the type of the data, most of the AH and BI data were monologues which the cheats ended with some sentences or one paragraph. The cheats initially introduced their business or need for help, and directly required the victims to accept their requests, and then offered the benefits of such businesses. The cheats in these data did not repair their speech, nor close it either. Interestingly, in the AH and BI data, when some receivers were curious or raised questions about the cheats' words, the cheats did not respond. The data indicated that all of the conversational frauds followed similar structures as follow:

1. Opening
2. Introduction about the purpose of chatting/pre-request
3. Narrating the problem
4. Officially requesting for help and making commitments to the victims
5. Closing (the cheats urged the addressees to take action to help them, or they kept questioning whether the victims were done with their task)

In conversational frauds, almost all the cheats started their talk by checking whether the victim was free to talk. Instead of greeting, most of them directly said 'There?' or 'Are you there?' While others were more direct and asked 'Are you free to help me?' or 'Do you have a minute to help me?' The most direct cheats said 'Do you have an e-bank account' or 'I need you to help me to transfer money.' Hence, it was observed that several cheats at this stage were very impatient. They had already stated their purposes or even problems before they received any response from the victims. After opening the conversation, the cheats began to introduce their purpose of chatting. Similarly, in the BI and SO data, except for several cheats who asked whether the victims owned an online bank account, other cheats directly explained the reason why they needed help. The reason could either be their friend/relative is in the hospital or they simply needed to transfer money to others. Most of the introductions of purpose are brief and ended with one sentence.

While some of the cheats stated their problems at the introductory stage, the others followed certain steps and after telling the victims they needed help, they would begin to explain what kind of help they were seeking. Right after the problem was narrated, the cheats officially put their request forward. Then, no matter what kind of excuses the victims presented, the cheats promised they would return the money soon. In closing their conversation, however, the cheat did not follow what Sacks (1975, p. 76) said: "A single conversation does not simply end abruptly, but it should be brought to a close." Therefore, when the conversation was going to end, the interlocutor should have signalled to their partners by saying 'I'll get back to you by tomorrow,' or 'I have to leave now.' Nevertheless, in the data of this study, no obvious pre-closing was observed. This does not mean the cheats were being rude, but it was well planned to encourage a quick response from the victims.

PRAGMATIC STRATEGIES

Pragmatically, the first few items to look into the data were in terms of Face Threatening Acts (FTA) and Politeness Strategy. The purpose was to find out whether the cheats respected the victims' expectations during the whole deception process. The need to be polite

can often account for why people choose to imply an idea rather than assert it directly (Peccei 1999). The cheats in all 50 data pieces never implied what they wanted. They were direct in their requests and did not address or redress any FTA (Face threatening acts). The FTAs and Politeness Strategy are therefore worthy of identification and explanation.

OPENING

Among the four types of politeness strategy, the bald on record strategy was applied when there was no effort to minimize threats to the receiver's face. The sender (cheats) performed direct speech acts containing imperatives with no mitigating device. This strategy was the most frequently applied strategy in this study.

Forms of address/greetings are products of social recognition of the addressee's age and social status. In most cultures, a greeting is a sign of politeness (Chiluwa 2009, Farashiyan & Tan 2012). And as Behnam and Amizadeh (2011) put it, compliments perform various functions but primarily and most obviously act as affective speech acts serving to increase or consolidate the solidarity between the speaker and the addressee. In the 50 QQ chatting records, no formal greetings were observed. Only in MT1, when the victim asked the cheat 'How's life', the cheat did answer 'Life's good', but in the rest of the records, the cheats utterances were direct and straight on in the openings. There were many examples of the bald on record strategy in the data. The opening formula in MT data was categorized and counted as an instance in Table 3.

TABLE 3. Opening formula in MT data

	Opening/greeting formula	Frequency	%
MT 1-2, 9, 11,13-14, 16, 17, 19, 20, 22, 27, 29	Opening as 'There?' or 'Are you there?'	13	44.8
MT 3, 6, 7, 12, 15, 23, 28	Opening as 'Do you have a minute?' 'Are you free to help me?' or 'I need you to help me transfer some money'	7	24.1
MT4-5, 21, 24	Opening as 'What are you doing?'	4	13.8
MT 8	Opening as sending video chat request	1	3.4
MT 10	Opening as 'Where are you?'	1	3.4
MT 18	Opening as 'Do you have e-bank account?'	1	3.4
MT 25	Opening as 'Dad. I carelessly dropped my phone in the toilet and it's broken.'	1	3.4
MT 26	Opening as' My purse is stolen, send me some money. My card number is xxxx'	1	3.4
	Total	29	

As Table 3 shows, what 44.8% of the cheats cared about was whether their victims were online or was able to chat by asking 'There?' or 'Are you there?' The word 'there' is abrupt as an opener to a conversation, and was not minimizing threats to the receiver's face at all. The data indicate that 13.8% of 'What are you doing?' and 3.4% of 'Where are you?' appeared hasty and abrupt as well. There is no respect or norms of address used; most of the cheats addressed the victims only as 'You' rather than by the victims' names. 24.1% of the cheats directly asked their target whether they were free to offer help. And in MT3 and 12, the cheats asked 'Do you have a minute? I need you to help me with something,' and 'Are you free to help me transfer money to my friend in China?'

In MT18, the cheats asked the victim "Do you have an e-bank account?" which is a direct question asking for personal information. It was thus, threatening the victim's negative face as well. To deal with this FTA, the cheats in MT18 pre-requested by saying that they had not asked for anything yet, and the victims at this point could refuse to answer but chose not to.

If FTA can be measured by size, then the largest size of FTA would be in MT26, 'My purse is stolen, send me some money'. The cheat in this case uttered an imperative sentence, and it left little opportunity for the victim to reject the request. An imperative expression is always categorized as the bald on record strategy. And, the sentence 'My card number is *******' is right after the previous utterance; notably to convince the victim of the cheat's intention. Though these words could increase the imposition on victims, it was working for the cheats.

Generally, the cheats utilized the bald on record strategy at the opening stage. Depending on different contexts, some of the strategies may be labelled as positive politeness strategy, but most of the cheats threatened the victims' negative face.

A complete absence of formal address pattern and greetings is noticed throughout the data, and most utterances take the form of imperatives to constrain the victims and to show authority over the victims. To interpret the cheats' politeness strategy, Brown and Levinson (1987) revealed that the bald on record strategy can also be oriented to saving the hearer's face, because directness often indicates a wish to be seen as socially close. Hence, the cheats relied on the intimate relationship between the real account owners and their respective victims.

INTRODUCTION ABOUT PURPOSE OF CHATTING/PRE-REQUEST

After checking on whether the victims were willing to talk, in this phase, the cheats started to claim they had something to discuss with the victims. Most of them consulted the victims and checked whether they could offer help. Once the victims answered them, they performed the request directly and kept pretending to be intimate with the victims.

As many of the cheats indicated to the victims that they were not in the QQ platform for chitchat, this part could be easily identified. Some of the cheats explained their purpose in the opening part, as in MT3, 6, 7, 12, and 15 as given in Table 3. In MT3, the cheat said 'Do you have a minute? I need you to help me with something.' The cheat in MT6 said 'Are you free to help me transfer money to my friend who is in China?' And in MT13, the cheat said, "Are you there? I have something urgent to tell you.'

To state the purpose at the beginning of a conversation would impose pressure on the victims. Despite this, the cheats clearly spoke of their needs. This type of opening could be undesirable even unwelcome to the victims. Especially in MT13, the word 'urgent' forced the victims to pay attention. Besides, the statement in MT3 'I need you to help me' appeared very haughty; and even if the cheats made up urgency, such an authoritative-like expression was inappropriate. Their acts undoubtedly threatened the victims' negative face. Thus, at this stage, the cheats applied the bald on record strategy.

PROBLEM NARRATION

The third phase within the whole deception process was to narrate the problems. Some cheats reversed the sequence of the problem narration and officially made their requests at the onset, which meant some cheats would inform the victims of their problem from the very beginning. Others follow an abrupt lead in and then narrated their problems. But this difference in order would not affect the politeness strategy the cheats applied. What is notable is that this phase was vital to the cheats. After stating their purpose, the cheats would assert various problems they faced, and asked for the victims' help. Table 4 categorises different types of problems that the cheats mentioned:

TABLE 4. Cheat's problem types

	Problem narration category	Frequency	%
MT 3, 9, 23, 26,	Reasons related to 'I don't have enough money'	4	13.8
MT 1, 2, 4, 5-8, 11-12, 15, 17, 18, 20- 22, 24, 28-29	Reasons related to 'My friend/relative needs money, but I'm too busy to leave/ I don't have enough money' or … 'My friend left foreign currency with me, he/she needs money now, but I'm not in China'	18	62
MT 13-14, 16, 19, 27,	Reasons related to 'I lost my bank card'.	5	17.2
MT 25	Reasons related to 'I need to pay my school fees'.	1	3
MT 10	No reason is stated	1	3

Table 4 illustrates the distribution of the problem types. Around 62% of the cheats stated their friends or relatives needed money, but due to certain reasons, they could not assist them. Although 13.8% of the cheats said they needed money themselves, 17.2% of them gave the same excuse but in a more stern tone. Only one cheat asked money for school fees and talked to the father of the original account owner and this was an isolated case. The cheat in MT10 was the only one that did not state any reason.

Except for the MT data, the cheats in the AH data also stated their problems; the cheat in AH1 said 'I'm helping my friend to test an online game and I need a QQ account…' and the cheat in AH2 said 'My friend joined Tencent New Silk Road Model competition…' These two cheats made their requests right after stating their reasons for chatting. In AH3, the cheat said '…Is she your classmate? I heard she is abroad? Where did you take the convocation photo? ...' to hint he/she has lost contact with 'her' in the speech. All the BI data were like advertisements, and the cheats mentioned standard words such as 'vacancy' and 'needed', and thus, did not arouse the suspicions of the victims.

The problem narration stage served as pre-request, and what the cheats expressed here was paving the way for the official request. Hence, it could be seen that all the cheats at this stage were performing the off-record strategy as they were going to threaten the victims' negative face, and further explanation would 'soften' the threats.

OFFICIAL REQUEST AND COMMITMENT

Most of the FTAs occurred in the official request and commitment stage, and this stage is considered the most 'offensive' stage. In contrast to the off-record strategy, there is more application of positive politeness as well as negative politeness on record and especially bald on record strategies. Although the cheats were the ones who were in need of help, most of requests were bold and without constraint. Table 5 presents the phrases cheats used in their requests:

TABLE 5. Cheats' request phrases

Data	Cheats' expression in request and promise
SO1	Help me buy something online, I'll return you the money later.
SO2	I want to buy something. Can you help me?
SO3	Help me buy antivirus software
SO4	Can you help me buy several cards? Help me buy online
SO5	I'm purchasing something online. Can you help me pay for it? I'll return you the money tomorrow.
SO6	Help me purchase something.
SO7	Ok, I want to purchase something, help me pay the bill, and I will return you the money by tomorrow,

Table 5 shows that each cheat's first-time request started with 'Can you help....' which appeared 3 times but a direct request, 'Help me ....' appeared 4 times. No tact in the choice of language such as 'Would you please' or 'Thank you' were discernible in the cheats'

speech. This kind of offensive request may have threatened the victims' negative face. In addition, there was no expression of gratitude or apology in any of the phases of the requests.

The cheats in SO3, SO4, and SO6 did not make any commitment to the victims, the victims in SO4 and SO6 discovered the cheats' identity, while the victim in SO3 was not capable of offering any help. Except for the cheat in SO2 who made commitment after various requests, the remaining 3 cheats made their commitments right after they make requests from the victims. The statement 'I will return the money tomorrow/later' meant to urge the victims to take action; thus, it was threatening the victims' positive face.

In contrast, the statement 'Can you help' came across as less direct than 'Help me ...', when the people directly expressed their needs; it can technically be described as being on record (Yule 1998), whereas the words 'Help me …' without using any terms of address for the victims can be seen as an imperative, so it is known as bald on record. Bald on record with direct command forms would be misleading, because imperative forms are often used by close acquaintances without being interpreted as commands (Yule 1998). The cheats' speech showed the cheats were either being very strategically aggressive or they lack politeness strategy.

CLOSING

Based on the observation of the 50 pieces of data, the last phase of the whole cheating process is closing. Unlike in emails, there is no proper closure by the cheats in this study. None of the cheats said or implied farewell to the victims. There were closing utterances to indicate farewell such as 'Thank you for helping me' or 'I'll talk to you later.'

In most of the MT and SO data, the cheats were busy urging the victims to offer help, or questioning whether the victims were done with their tasks. Thus, the closing stage may be considered as the expansion of the request. In the BI data, the monologue ended with invitation codes to make their words more believable and formal. The AH data usually ended with the QQ account information given freely to the cheats. Because of the various expressions and attitudes that the cheats presented at this phase, it was sometimes hard to categorize their speech. In these cases, the cheats acted like they had the right to give orders to the victims; in fact, their request was an intrusion into the victims' privacy and void of respect. Due to the fact that the language that cheats used was direct and face threatening, the politeness strategies applied in this stage were largely bald-on record and less, on record strategies.

SPEECH ACTS

In attempting to decode how the cheats proceeded with their deceptive behaviour, the researchers studied the speech acts of the cheats' utterances.

OPENING

At this stage, their speech acts mostly were questioning, ordering, and requesting. Rather than simply making a request, in the data of MT and SO, almost all of the cheats made pre-requests. Here are some examples:

(SO4) There? Do you have an e-bank?
(SO6) Did you open an online bank?
(SO7) Do you have an online bank account?
(MT4) Mom, what are you doing?
(MT20) There? What are you doing bro?

The data indicate that 44.8% of the cheats cared about whether their target was online or was able to chat by asking 'There?' or 'Are you there?' Examples above show another kind of opening: these cheats either questioned the victims' privacy or their activity at the moment. The surface act the cheats performed was questioning. However, their intention was not just asking a question but inviting the receiver to join the conversation. Therefore, the cheats' illocutionary acts can be seen as inviting. After they've performed the action of inviting, the perlocutionary act they would receive was a response from the victims.

As Austin (1962) defined, illocutionary act refers to speaker's intention in producing an utterance, and perlocutionary act is the effect of the utterance uttered to the hearer. Each of the cheats' speech was multifunctional, and simultaneously was preparing for further conversation. Their directive and expressive acts affected the victim in such a way that they became concerned about the issues the cheats made up, and the fact that the issues were serious and urgent. For example:

(AH2) By the way, can you help me for two minutes?
(SO1) Have you a registered Visa card and e-Bank?
(SO2) I want to ask you something. Can you shop online?

NARRATION OF THE PROBLEMS

After introducing their purpose, the cheats would point out various problems hindering them from transferring money. According to Chiluwa (2010), in pragmatic theory, every sentence/utterance has implied meaning, and it is quite easy to see how the cheats performed representative acts while narrating long stretches of events.

Among the 29 pieces of MT data, 66% of the cheats chose excuses such as their friends or relatives were in trouble, and that they did not have enough money or they could not leave at the moment; hence, they needed the victim to help them. These cheats' illocutionary speech acts were directives and representatives, specifically in claiming, stating, requesting, and convincing. The following 17% data referred to another excuse which was 'lost personal bank card,' and they wanted to transfer their money to the victim. Rather than borrowing money from the victims, the cheats wanted to give money to the victims. Nevertheless, they actually intended to get the victims' personal information such as bank account number, IC number, as well as phone number. Therefore, directive and representative speech acts were observed.

OFFICIAL REQUEST AND COMMITMENT

The official request and commitment stage was the stage of directive and commissive speech act and the cheats directly asked the victims to transfer money, or requested them to do things they wanted. Accordingly, the cheats made a series of requests because the victims might hesitate to offer help. Some of the cheats made the requests first and then promised they would return the money, whereas the others would commit first and then kept urging the victims to take action. Whether or not the victims were willing to help, the cheats consistently showed their commitment by saying they would return the money.

(AH1) Lend your QQ account to me for a while ok? Just two minutes.
(AH2) Help me to vote for her.
(AH3) Open the website I sent to you, there are some of her photos, the convocation photos.
(MT2) How much money do you have now? Do you have 5000?
(MT3) I want you to help me transfer some payment.
(MT6) I'll give you my internal friend's card account, and you help me to deposit the money. My friend needs the money now. What kind of bank do you have near your house?

The cheats' speech showed that they did not use words such as 'please' or 'thank you' at all; they made their impatient requests with a sense of urgency. They typed sentences like 'Just help me to deposit the money,' and 'Help me to vote for her.' However, the person that the cheat pretended to be was of equal social status with the victims. In this sense, the cheats were just emphasizing their solidarity. Some of the cheats made promises right after they requested for money, while others promised the victims after several turns in the conversation. When the victims said that they did not have enough money or they were busy, the cheats would keep on resorting to the speech acts of performing, convincing, requesting, comforting and slightly threatening the victims. Instances are shown below:

(AH1): Is that OK?! You don't need to close your QQ, you can still chat with your friends, I just need two minutes.
(MT2): I'll return you the money later
(MT 3): I will return the money the day after tomorrow. Yep, no worries just help me to deposit 3000 yuan sharp.

CLOSING

Closing and sign offs generally perform expressive speech acts (Chiluwa 2010). Based on the observation of the 50 pieces of data, the last phase of the whole cheating process was closing. Unlike writing an email, not all the cheats closed the conversation officially. Most of the cheats did not say goodbye to the victims; there was no such statement as 'Thank you for helping me' or 'I'll talk to you later.' In the BI data, the monologue ended with an invitation code to make their intention believable and formal.

(BI 1) Invitation code: 557
(BI 2) And the invitation code of our group is 382. Without invitation code, it is prohibited to join!
(BI6) Required code: 333 (compulsory)

Except for SO2, MT15, and MT25, the rest of the cheats were all seen through at this stage, and they realized that the victims were not going to send the money to them. Interestingly, they still insisted on convincing rather than giving up. Noticeably, the cheats who succeeded in cheating were concerned about being informed by the victims of the status of the money transfer, and they focused on 'After you have transferred the money, tell me online.' And the cheats who failed in deception would keep emphasizing the problem, and attempted to regain the victims' trust. Their illocutionary acts were still convincing, requesting, and threatening. An emphasis on the seriousness of the problem could startle the victim and encourage them to offer help. In SO2, the victim believed the cheat; therefore, the cheat's request to be informed when shopping was done was fulfilled as a directive speech act. Consequently, because this phase was the expansion of the official request phase, the directive speech acts still rank highest among the speech acts.

FURTHER DISCUSSION

Focusing on how people are deceived into revealing their bank details or transferring money to the cyber cheats' accounts, the researchers collected 50 instances of online conversations of such nature between the cheats and victims. Since the source texts were in Chinese, the whole discourse was translated into English and then was examined from different aspects. For example, it was explored how the framing of each discourse structure took, what speech acts were employed and what strategies were used to win the victims' trust.

The data showed that all the cheats knew how to create a friendly chatting atmosphere in order to win trust. Generally, the cheats' flow of modus operandi starts with making up a story and asking for money, fixing their lies when the victims raised doubts, and eventually

convincing the victims into doing what they wanted. Since the cheats were pretending to be the victims' friends, the chats were casual. Although most of the conversations were structured as (i) opening, (ii) chatting, and (iii) closing, many of them did not get a clear close at the end, either because the cheats were discovered by the victims at this stage or they urged the victims to take action, bringing the conversation to an abrupt end. Given this, the cheats had cleverly planned the frauds and used language in a particular way to deceive the victims.

Pragmatically, there was no effort provided to minimize threats to the receiver's face as there were no mitigating devices employed. The data indicated that there was a complete lack of formal address pattern and greetings, and most utterances took the form of the imperatives to constrain the victims. In addition, the speech acts as formulated by Searl (1979) were identified in the cheats' discourse. They included expressive, representative, commissive and directive acts.

Referring to the study conducted by Maros and Rosli (2017) which focused on the employment of politeness strategies in Twitter updates and found that positive politeness to be the most frequently used politeness strategy by female Twitter users, the present research revealed that this strategy was common as well, particularly in the opening messages.

Similar to hoax emails, this study showed pragmatic strategies both in structure and content of the chatting records, which indeed had an impact on cheats' acts of requesting. To compare with the hoax email writers, the cheats in instant communication appeared more aggressive and imperative. This feature can also be spotted in the study conducted by Kiang (2003), who made use of a corpus comprising 102 electronic mail messages from the executives' routine communication in work contexts where there was a predominance of main clauses in imperative and declarative moods, and subordinate clauses denoting purpose and reason. This may reflect that e-mail communication of the community is used more for requesting and informing, and less for enquiring unlike instant messaging.

CONCLUSION

This study has demonstrated that a certain discourse pattern on the way cheats or fraudsters follow to steal money is discernible and the language they use is formulaic. The findings contribute substantially towards developing a model of cheat discourse structure, which can possibly raise awareness among cyber users of such rampant crimes. It should also be emphasised that the victim's vulnerability to such lies and the reasons behind them deserve a closer examination by language scholars and the cyber community at large.

REFERENCES

Austin, J. (1962). *How to Do Things with Words*. Oxford: Oxford University.

Behnam, B., & Amizadeh, N. (2011). A comparative study of the compliments and compliment responses between English and Persian TV interviews. *3L: The Southeast Asian Journal of English Language Studies. Vol. 17*(1), 65-78.

Blommaert, J. (2005). Making millions: English, indexicality and Fraud. *Working Papers in Urban Language and Literacies*.

Brown, P. & Levinson, S. (1987). *Politeness*. Cambridge: Cambridge University Press.

Chiluwa, I. (2010). The pragmatics of hoax email business proposals. *Linguistic Online. Vol. 43*

Chiluwa, I. (2009). Discourse of digital deceptions and 419 email. *Discourse. Vol. 11*, 635-636.

Chun-tao, G. U. O. (2011). Shallow research on the concept, main forms and crime constitute of Internet fraud [J]. *Netinfo Security. Vol. 4,* 28-35.

Coleman, L. & Kay, P. (1981). Prototype semantics: The English word lie. *Language*, 26-44.

Ekaning K. (2011). Pragmatic competence in the spoken English classroom. *Indonesian Journal of Applied Linguistics. Vol. 1*(1).

Galanxhi, H. & Fiona Fui-Hoon Nah. (2007). Deception in cyberspace: A comparison of text-only vs, avatar-supported medium. *Int. J. Human-Computer Studies. Vol. 65,* 770-783.

Hancock, J. T. (2007). *Digital Deception. Oxford Handbook of Internet Psychology*. 289-301.

Hancock, J. T., Curry. L. E., Goorha, S. & Woodworth, M. (2008). On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes*.

Herring. S. C., Stein, D. & Virtanen, T. (Eds.) (2013). Introduction to pragmatics of computer-mediated communication. *Handbook of Pragmatics of Computer-mediated Communication.* 3-31.

Huang Yang (2007). *Pragmatics*. Oxford Press.

Kiang, N. Y. (2003). A discourse analysis of e-mail messages in a Malaysian business community. *GEMA Online® Journal of Language Studies. Vol. 3*(1).

Lu, Y., Zhou, T. & Wang, B. (2009). Exploring Chinese users' acceptance of instant messaging using the theory of planned behavior, the technology acceptance model, and the flow theory. *Computers in Human Behavior. Vol. 25*(1), 29-39.

Maros, M., & Rosli, L. (2017). Politeness strategies in Twitter updates of female English language studies Malaysian undergraduates. *3L: The Southeast Asian Journal of English Language Studies. Vol. 23*(1).

McCarthy, P. M., Duran, N. D. & Booker, L. M. (2012). Devil is in the details: New directions in deception analysis. *Proceedings of the Twenty-Fifth International Florida Artificial Intelligence Research Society Conference Publication*.

O'Keeffe, A., Clancy, B. & Adolphs, S. (2011). *Introducing pragmatics in Use*. Routledge Taylorand Francis Group Publications.

Peccei, J. S. (1999). *Pragmatics*. Routledge Taylorand Francis Group.

Robichaud, A. & Blevins, C. (2011). Tooling up for digital humanities. *Journal of Information Systems. Vol. 20*(1), 69-92.

Sacks, H. (1975). *Everyone Has to Lie. Sociocultural Dimensions of Language Use.*

Satu Elo & Helvi Kyngas. (2007). The qualitative content analysis process. *Journal of Advanced Nursing. Vol. 1,* 107-115.

Searl, J. R. (1979). *Expression and Meaning*, Cambridge University Press.

Tan, K. H. & Woods, P. (2008) Media-related or generic-related features in electronic dictionaries: Learners' perception and preferences. *GEMA Online® Journal of Language Studies. Vol. 8*(2), 1-17.

Tan, K. H. & Farashiyan, A. (2012) The effectiveness of teaching formulaic politeness strategies in making request to undergraduates in an ESL classroom. *Asian Social Science. Vol. 8*(15), 189-197.

Yule G. (1998). *Syntax, Semantics, and Pragmatics.* Pragmatics.

Yunus, M. M. et al. (2007). Language learning via ICT: Uses, challenges and issues. *Journal WSEAS Transactions on Information Science Applications*. *Vol. 6*(9), 1453-1467.

Zhou, L. et al. (2003). An exploratory study into deception detection in text-based computer-mediated communication. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, IEEE,* 10.

Zhou, L. & Sung, Y.W. (2008). Cues to deception in online Chinese groups. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, IEEE,* 146-146.

Zhou, L. & Zhang, D. (2004). Can online behavior unveil deceivers? An exploratory investigation of deception in instant messaging, *1EEE.*

Zhou, L., et al. (2003). An exploratory study into deception detection in text-based computer-mediated communication. In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference, IEEE,* 10.