2024

Scammer Strategies and Social Actions in Online Filipino Transactions

Kiarah Reyshylle C. Ibañez

Date received: October 9, 2023
Date revised: February 1, 2024
Date accepted: March 6, 2024
Similarity index: 3%

Abstract

As technology has developed newer and faster forms of communication, the internet has also become a convenient medium for scammers to interact with their targets. Since deception is understudied from a linguistic perspective, this paper investigated the persuasive strategies and linguistic markers of scammers and analyzed the social actions of both scammers and their targets— all of whom are users of the Filipino language. This qualitative study employed digital conversation analysis in analyzing ten conversations between scammers and their targets, which were all failed scams. The results showed that scammers used emotion, credibility, and logic in persuading their targets. The following linguistic markers were found in their utterances: (1) pronouns that are personal, exclusive, inclusive, noncommittal, impersonal, and ambiguous; (2) negation used for denial, non-existence, refusal, discouragement, inability, loss, contrast, clarification, and correction; (3) emotion words expressing happiness, astonishment or amusement, worry, doubt or fear, shame, regret or inadequacy, and fondness, and lastly, (4) cognitive verbs indicating equivocation, and expression of knowledge or understanding. Furthermore, the social actions of the scammers and the targets were categorized into four sequences that generally involved certain actions: (1) pre-offer (asking about and providing details), (2) insert (expressing doubt and explaining), (3) offer (offering or asking for money/info, and rejecting), and (4) post-offer (insisting, showing aggression, or conceding and retaliating or interrogating). Although all conversations resulted in the targets' rejection of the scammers' offer, which undermines social solidarity, dispreference is seen as a beneficial response in conversations involving scams.

Keywords: conversation analysis, persuasive strategies, deceptive strategies, preference organization, online scams

Author Information:

Kiarah Reyshylle C. Ibañez
krcibanez.linguistics@gmail.com
orcid.org/0000-0002-4605-0391

Teacher
Senior High School,
Mati National Comprehensive High School,
Mati City, Davao Oriental, Philippines

https://doi.org/10.53899/spjrd.v29i1.287

Communication nowadays is not only limited to traditional face-to-face exchanges but also virtual interactions. Although technology is a valuable tool in conversations, scammers have exploited online chats to prey on their targets. In such conversations, language use is deceptive. However, in comparison to speaking, deception is easier in writing as it allows the writer to plan the lie strategically (Picornell, 2013). Despite being a common phenomenon, only a few linguistic studies have been conducted to analyze deception (Meibauer, 2018). These studies revolved around email spam (Schaffer, 2012), sex predation (Chiang & Grant, 2018), and romance (Shaari et al., 2019). Since understanding deception in these mediated contexts is important as it occurs in a wide range of activities— from sexual predation to financial scams (Hancock et al., 2008), the lack of research on the latter stresses the need to analyze deception in online business transactions. This paper aims to analyze the persuasive strategies used by scammers, their deceptive strategies based on their linguistic markers, and the social actions of both the scammers and their targets as found in their online conversations to address this gap.

As stated by Beebe and Beebe (2012), there are three ways that a speaker can persuade his or her audience based on Aristotle's modes of persuasion: enhancing credibility (ethos), using logic and evidence (logos), and using emotion (pathos). Credibility can be enhanced by demonstrating competence, trustworthiness, and dynamism, while logic is used by providing evidence (e.g., facts, examples, statistics, and expert opinions) to support one's reasoning (i.e., causal, deductive, inductive, and reasoning by analogy). Lastly, an emotional appeal can be done using concrete examples for visualization, emotion-arousing words, nonverbal behavior to communicate emotional response, visual images to evoke emotions, appropriate metaphors and similes; fear appeals, appeals to one's values, and people's beliefs in myths.

This persuasion can be the onset of deception (Handoko et al., 2015). According to Picornell (2012), two classifications of liars can be identified based on their linguistic markers: (1) personal and prolix, and (2) impersonal. The first one is characterized by verbose, highly personal (i.e., frequent use of first-person singular pronouns), and noncommittal language use (i.e., use of negation, cognitive verbs, verb strings, and indefinite pronouns), while the latter is marked by direct and other-oriented language use (i.e., increasing use of third-person or first-person plural pronouns as a gradual replacement to first-person singular pronouns).

Moreover, deceptive accounts are usually marked by fewer first-singular and third-person pronouns, fewer exclusive words, more negative emotion words, and more motion words (Newman et al., 2003). Dou et al. (2017) also added that liars use noncommittal phrases or ambiguous expressions to indicate their lack of commitment to their statements. These deceptive communications also involve extraneous details, moderating adverbs (Sandoval et al., 2015), equivocation or linguistic hedges, and non-prompted negation or negative expressions (Choudhury, 2014; Sandoval et al., 2015).

The progression of deception is analyzed to examine how participants in a conversation exchange utterances, while the liar develops their deception and the recipient, deals with such action. These social actions are considered the "performative aspects" of talk (Lester & O'Reilly, 2019), which refer to the way people do things with their language, like asking, inviting, complaining, apologizing, and others (Drew, 2013).

In a conversation, a two-part exchange of messages is composed of actions, in which the first pair part (FPP) is the sequence-initiating action (i.e., the initial utterance that requires a response) while the second pair part (SPP) is the sequence-responding action (i.e., the response to the previous utterance) (Schegloff, 2007). This base pair may come with multiple expansions: pre-expansion (expansion of pre-sequences before the base FPP), insert expansion (expansion of insert sequences after the base FPP and before the base SPP), and post-expansion (expansion of post sequences after

the base SPP). These sequences are marked by the subscripts "pre," "ins," and "post," respectively (Schegloff, 2007, p. 27).

In various deceptive communications, Schaffer (2012) stated that common actions in email spam are apologizing, flattering, making the recipient curious, appealing to emotions, using attention-grabbing words (e.g., urgent, secret), and committing errors. Additionally, Chiang and Grant (2018) described that an online groomer's actions include greeting their victim, establishing rapport, assessing and managing risk, maintaining conversation, performing sexual moves, planning the meet-up, reprimanding, and signing off. Similar results were discussed by Shaari et al. (2019), who claimed that online romance scams involve the following actions: setting up contact, establishing relationships, gaining trust, developing personal relationships, grooming, maintaining the relationship, presenting the bait, and asking for money.

In investigating this issue, this paper analyzed how online scammers interact with their targets by doing a digital conversation analysis to recognize the rise of virtual environments and the need for conversation analyses in these contexts (Giles et al., 2015). Through the analysis of fraudulent conversations from a linguistic standpoint, this research was conducted to help address the growing concern over financial scams in the digital era.

Materials and Methods

This research is a qualitative study employing digital conversation analysis. A digital conversation analysis is a methodological approach to the study of durable forms of online interaction that further the study of talks through various media (Giles et al., 2015). According to Meredith (2015), digital CA involves the collection of naturally occurring data that are available in the online environment. With this, the study exhausted the available data online. It included only those conversations that have been given consent by the post owners or targets who claimed and verified that the transactions were scams, which all turned out to be failed scams as posted by the targets. For these reasons, this paper analyzed the 10 available conversations posted on Facebook from July 2020 to July 2022. The use of Facebook as a platform source for this study was based on a similar study conducted by Shaari et al. (2019), which involved the analysis of online conversations between scammers and victims and gathered data from Facebook as a social media platform.

Since sampling in CA is purposive (Lester & O'Reilly, 2019; ten Have, 2007), the research corpus of this study was selected and collected by the researcher based on the following criteria: (1) the conversations between the scammers and their targets involved money and fraudulent interaction, (2) the conversations primarily used English and involved Filipinos as evident in the occasional use of Filipino language and mention of the Philippine peso currency, (3) the conversation had at least ten turns (a turn refers to an interlocutor's chance to send a message until the other interlocutor takes the floor) as the length of the interaction plays a factor in examining the progression of both the persuasive and deceptive strategies in the online chats, and (4) the posted chats were verified by the post owners as scams.

In referring to the interlocutors conversing with the scammers, this paper used the term "target" to suggest neutrality (PACER's National Bullying Prevention Center, 2018) and indicate that such individuals were not victimized by the scammers. These chats involved Filipino speakers, as evidenced by their use and understanding of Filipino and their reference to the Philippine peso as the currency of payment.

Although this study is qualitative, this paper included the frequency and percentage of research findings to present internal generalizations or the generalizability of the conclusions within the context

of the study (Maxwell, 2021). The research corpus comprises 10 conversations with 5,641 words, 47 emojis, 21 pictures, and 13 links. These online conversations are considered naturally occurring data since they involve no intervention from a researcher (Meredith & Potter, 2014).

In analyzing the data, Beebe and Beebe's theory on persuasive strategies (2012) was utilized to determine how scammers use emotion, logic and evidence, or their credibility in convincing their targets. Moreover, Picornell's theory on deceptive strategies (2012) was used to examine the scammers' linguistic markers, particularly their use of pronouns, negation, emotion words, and cognitive markers. Lastly, Schegloff's theory on preference organization (2007) was employed to analyze the social actions of the interlocutors and the dispreferred responses.

The analysis of the study was reviewed and validated by three faculty members in linguistics in the Davao Region, Philippines: a college professor at a private university in Davao City, an associate professor at a state college in Davao del Norte, and an instructor at a private university in Davao City. The validators reviewed the manuscript using the validation sheet, incorporating their comments and suggestions.

Results and Discussion

Digital platforms offer a growing repertoire of linguistic data and social interactions that can be used to analyze conversations. Since conversations are done for different purposes, this study focuses on the deceptive use of language in online scams.

Persuasive Strategies of Online Scammers

The results of this study revealed that scammers employed persuasion in online business transactions using different modes: using emotion (pathos), enhancing credibility (ethos), and using logic and evidence (logos) (Beebe & Beebe, 2012). In particular, scammers used the following sub-strategies that were mentioned in Beebe and Beebe's theory (2012): (a) in using emotion, scammers used emotion-arousing words, fear appeal, appeal to one's values, and beliefs in myths; (b) in enhancing credibility, scammers used trustworthiness and competence; and (c) in using logic and evidence, scammers used causal reasoning.

Aside from these, certain findings that were not mentioned in Beebe and Beebe's theory (2012) also emerged from the research corpus and revealed the scammers' use of other sub-strategies: appeal to flattery, pressure appeal, appeal to greed, appeal to connection, appeal to sympathy or pity, which are all categorized as emotional appeal, and bandwagon as a sub-strategy in using logic and evidence. The following table shows the specific strategies scammers use to persuade their targets:

DOI: https://doi.org/10.53899/spjrd.v29i1.287

Table 1

Persuasive Strategies of Online Scammers

Strategy	Sub-strategy	f	%	Sample Excerpt
Using Emotion (Pathos)	Emotion-arousing Words	92	41.1	"I assure and guarantee you that this is 100% legit"
	Appeal to Flattery	31	13.8	"sir any problem ??" "okay okay i am waiting sir"
	Pressure Appeal	17	7.6	"YOU WILL RECEIVE A NEW CODE NOW IMMEDIATELY YOU GET THE CODE SEND IT TO US BEFORE IT['S TOO] LATE OKAY"
	Appeal to One's Values	15	6.7	"I WILL ADVICE YOU TO BE VERY LOYAL AND HONEST WITH US SO THAT WE CAN GET TO YOUR DESTINATION"
	Appeal to Greed	12	5.4	"The minimum here is 100$ which is 5k pesos then at the end of Tomorrow which is currently 9pm you withdraw 51k to your Gcash madam"
	Appeal to Connection	8	3.6	"Hi. I just thought I would say hello and see how you?"
	Fear Appeal	5	2.2	"Or else your account will be disabled and locked out"
	Appeal to Sympathy or Pity	5	2.2	"I understand you I'd have love to but it could affect my trade and that could lead too lost"
	Beliefs in Myths	1	0.4	"Doubts kills dreams faster than failure will"
Enhancing Credibility (Ethos)	Trustworthiness	19	8.5	"I'M AGENT [X44], the 2021 FEDERAL GOVERNMENT WINNING APPEAL BOARD GENERAL AGENT…"
	Competence	3	1.3	"My company makes use of Mining Machine Which generates Bitcoin after every transaction that is connected to the trends of the trading signals _ THE AUTO –AUM pattern helps in reading the waves of the signals so that direct us to enable the outcome of the profit from every investment"
Using Logic and Evidence (Logos)	Causal Reasoning	12	5.4	"You have to deposit 5k into your gcash wallet to get started with your trading"
	Bandwagon	4	1.8	"I thought you invested because most people message me because of investment"
Total		**224**		

Using Emotion as a Persuasive Strategy of Online Scammers

The most common strategy scammers use to persuade their targets is emotional appeal. This is done by appealing to their emotions, such as excitement, happiness, pressure, fear, and sympathy.

Emotion-arousing Words. The majority of the scammers aroused their targets' emotions through words by ensuring security using expressions like "I assure and guarantee," "100% legit," "secure/secured/totally secure," and "legit/legitimate," as shown in Figure 1.

Figure 1

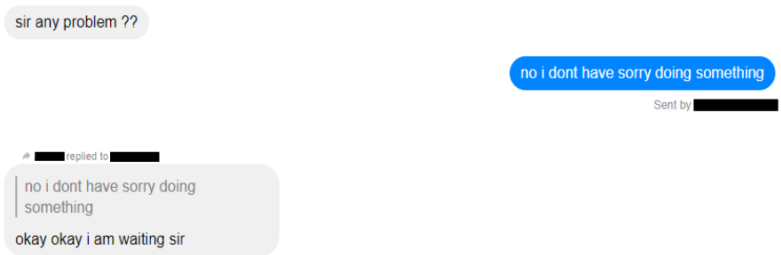
Emotion-arousing Words

Aside from ensuring security, scammers also use emotion-arousing words by emphasizing benefits, like "free," "efficient/time efficient," "transparent/very transparent," "flexible," and "profitable," 3) announcing winnings using "congrats/wow congrats," "dear winner," "lucky" and "winnings/winning," and 4) indicating eligibility using words like "accepted," "eligible," and "successfully" to encourage the targets to continue making progress.

Appeal to Flattery. Although flattery is done by complimenting the good qualities of a person, scammers appeal to flattery through the repetitive use of polite forms of address, such as "sir" (as shown in figure 2), "madam/ma'am," and the use of Filipino polite expression "po," to make the targets feel superior and respected.

Figure 2

Appeal to Flattery

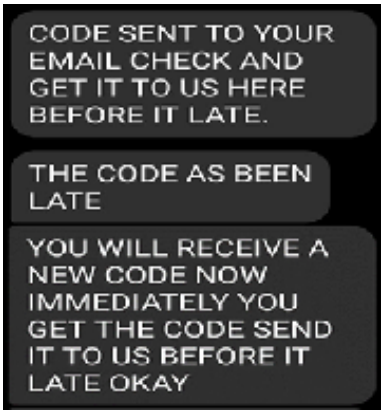


Pressure Appeal. Pressure appeal is done when an individual makes another person feel pressured in order to manipulate them. A sample of this is shown in Figure 3.

DOI: https://doi.org/10.53899/spjrd.v29i1.287

Figure 3

Pressure Appeal

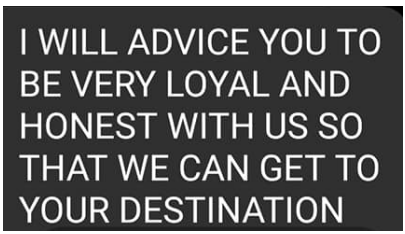


Expressions like "before it('s too) late," "now/right now," "immediately/immediate," "very important," and "without any delay" are used to demand immediate action. Interestingly, farewells, such as "Have a nice day" and "goodbye," are also used as passive persuasion to indirectly pressure the target that non-compliance might result in losing their chance to earn.

Appeal to One's Values. Values and beliefs are things that people hold dearly. However, some scammers use and exploit such things to gain a favorable response.

Figure 4

Appeal to One's Values

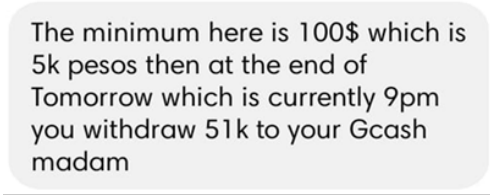


The following expressions are used to appeal to certain values: (a) advising to be "very loyal and honest" (as shown in figure 4) to seek cooperation, (b) encouraging to "support for COVID-19" and support one's "family" to promote helpfulness, (c) saying that "it's left for you to decide" to encourage risk-taking and (d) using the phrase "Almighty God" to express faith.

Appeal to Greed. Scammers appeal to the target's greed in various ways. One of their ways is to offer easy money by asking for a small investment in exchange for a relatively huge profit in a short span of time, as shown in Figure 5.

Figure 5

Appeal to Greed

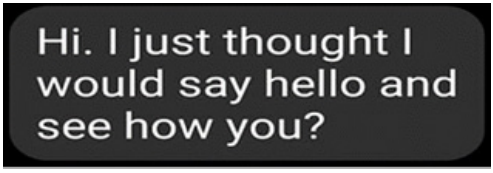


Another way is to flaunt their earnings (usually with screenshots as proof of one's earnings) to encourage the target to follow. Lastly, some scammers present lottery prizes to lure the target into providing their payment or personal information.

Appeal to Connection. Scammers connect to their targets in two ways: 1) creating a friendly atmosphere by using greetings, welcoming attitude (as shown in figure 6), gratitude, and less formal talk, and 2) using terms of endearment, such as "dear" and "sister."

Figure 6

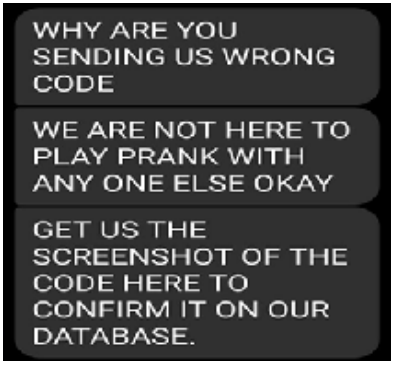
Appeal to Connection



Fear Appeal. Fear appeal is done by displaying anger or aggression, as in "we are not here to play a prank," as shown in Figure 7.

Figure 7

Fear Appeal



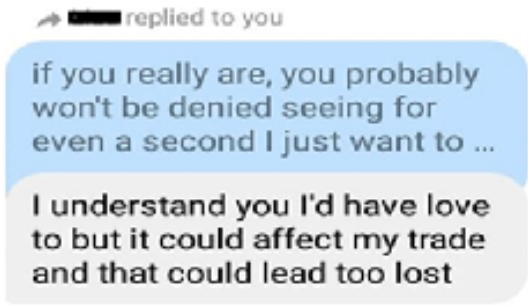
DOI: https://doi.org/10.53899/spjrd.v29i1.287

Another way they impose fear involves threatening, which is by asking the target to follow the scammer's instructions. Otherwise, they will face a negative consequence, such as "your account will be disabled and locked out."

Appeal to Sympathy or Pity. Appealing to pity is specifically done by scammers by expressing their understanding of the target's situation, as shown in Figure 8.

Figure 8

Appeal to Sympathy or Pity

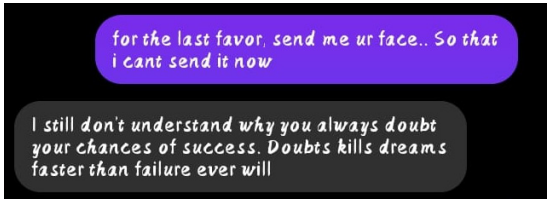


Aside from expressing their understanding, scammers also use disclaimers like "am not the best/professional but" to lower the target's expectations and emphasize their willingness to help despite their humble position or situation.

Beliefs in Myths. This is done by appealing to the target's beliefs in myths—or false and widely-held beliefs, as shown in Figure 9.

Figure 9

Beliefs in Myths



The scammer stated that "doubts kill dreams faster than failure," suggesting that failing is better than being afraid to take risks and losing the chance to succeed. This was the scammer's attempt to encourage the target to disregard the dangers that might come with doubts.

Enhancing Credibility as a Persuasive Strategy of Online Scammers

Scammers enhance their believability by earning their targets' trust and showing their own competence. This is usually done by showing supporting documents or proofs and providing technical explanations to make themselves appear credible.

Trustworthiness. One of the ways that scammers use to prove their trustworthiness is by presenting proofs (e.g., certificates, licenses, testimonies), as shown in Figure 10.

Figure 10

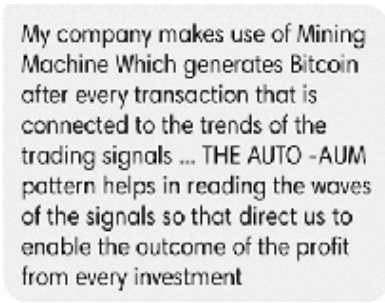
Showing Trustworthiness

When the target asked for documents as proof, the scammer presented their license or business certificate to show that the business was legitimate. Scammers use documents like this as evidence to gain their targets' trust.

Competence. Scammers show competence by exhibiting their skills as they perform a certain role. Certain scammers provide lengthy explanations using technical terms to demonstrate their competence, as shown in Figure 11.

Figure 11

Showing Competence



Aside from demonstrating their technical knowledge, one scammer showed competence by explaining one's flexible roles as a "life coach, budding writer, market analyst, and expert trader."

Using Logic and Evidence as a Persuasive Strategy of Online Scammers

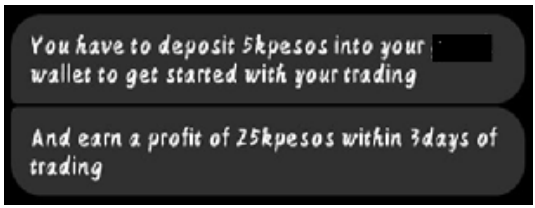
Scammers use logic to convince their targets, particularly through causal reasoning and bandwagon appeal. The former is done by presenting the cause and effect of their offer, and the latter is by using the majority as an example to persuade the target.

DOI: https://doi.org/10.53899/spjrd.v29i1.287

Causal Reasoning. The necessary cause is often emphasized to deceive the target to try such a cause and enjoy the benefits of the results, as shown in Figure 12.

Figure 12

Causal Reasoning

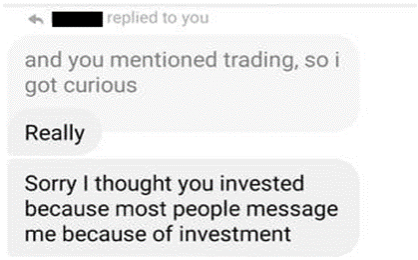


The scammer convinces the target to "deposit 5,000 pesos" in their mobile wallet (necessary cause) in order to "get started with trading and earn a profit of 25,000 pesos within three days of trading" (predicted result). By presenting these premises, the scammer persuaded the target to do the former (cause) in order to achieve the latter (effect).

Bandwagon. Scammers use bandwagon by referring to the majority as an example and encourage the target to jump on the bandwagon to reap the benefits many people have experienced.

Figure 13

Bandwagon



As shown in Figure 13, the scammer used the expression, "Sorry, I thought you invested because most people message me because of investment," to indicate that many people have been involved in such investment and persuade the target to do the same.

Linguistic Markers of Online Scammers

This paper analyzes their persuasive and deceptive strategies based on their linguistic markers to understand the deceptive language of scammers. The following are the particular findings of the study based on the scammers' use of pronouns (that refer to themselves or the people who may be involved in the scam), negation, emotion words, and cognitive verbs.

Table 2

Linguistic Markers of Online Scammers

Markers	Sub-markers	f	%	Sample Excerpt
Pronouns	Personal, Exclusive, and Inclusive	104	44.6	"[1]Firstly I will like to know your name and your country eligibility before we proceed further? [2]Your country nationality is accepted with our company broker system"
	Noncommittal	38	16.3	"[1]They compensate me $50,000 when i apply for it the money is free which i won't have to pay it back,did you get yours from them too? [2]CONGRATULATIONS OUR DEAR WINNER IS NAME WAS CHOSEN AS ONE OF OUR LUCKY WINNER WHO WON FROM FACEBOOK…"
	Personal and Exclusive	34	14.6	"We are using this priviledge, so you can support your family due to pandemic covid19. I am delighted to inform you that your account on Instagram was luckily…"
	Impersonal	21	9.0	"[1] This is trade I invested with [name of a person] [2]And she help me earned"
	Personal and Inclusive	20	8.6	"I believe we should be able to maintain a long term business relationship…."
	Highly Personal	15	6.4	"You go to register, I will transfer 10USDT to your registered account, you follow my uncle's trading signals…"
	Ambiguous	1	0.4	"…We need to update your account on the main system to avoid error and delayed transaction…"
Total		**223**		
Negation	Denial	28	35.9	"I'm not a scammer madam"
	Non-existence	14	17.9	"no experience is needed"
	Refusal	12	15.4	"No borrow here you can borrow from your friends…"
	Discouragement	9	11.5	"it is not better for you to study it yourself"
	Inability	5	6.4	"I don't understand you"
	Loss	4	5.1	"…it disconnect the company system"
	Contrast	3	3.8	"Are you interested or not madam?"
	Clarification	2	2.6	"Are you not a student?"
	Correction	1	1.3	"No, what can I do for you"
Total		**78**		

Markers	Sub-markers	f	%	Sample Excerpt
Emotion Words	Happiness, Astonishment, or Amusement	12	42.9	"CONGRATULATIONS!!!
	Worry, Doubt, or Fear	7	25.0	"You don't have to be scared…"
	Shame, Regret, or Inadequacy	7	25.0	"Sorry I thought you invested…"
	Fondness	2	7.1	"I'd have love to but it could affect my trade…"
Total		**28**		
Cognitive Verbs	Equivocation	6	54.5	"I believe we should be able to maintain long term business relationship…."
	Expression of Knowledge or Understanding	5	45.5	"sir i don't know"
Total		**11**		

Pronouns as Linguistic Markers Used by Scammers

Picornell (2012) classified pronoun usage to be either 1) prolix and personal or 2) impersonal. In addition, the following emergent findings were found on the scammers' pronoun usage: exclusive and inclusive use of first-person plural pronouns, noncommittal language (Dou et al., 2017), and ambiguous pronouns (Bal & Stone, 2021; Kapelke-Dale, 2021).

Personal, Exclusive, and Inclusive. This is the most common set of pronouns the scammers use in the research corpus. One sample is shown in Figure 14.

Figure 14

Personal, Exclusive, and Inclusive Pronoun Usage

As shown, it involves the use of various pronouns: (a) first-person singular pronouns as personal pronouns as in "I will like to know you" to express one's personal desire; (b) first-person plural pronouns as an exclusive pronoun, as in "our company" to refer to the scammer's exclusive membership to a certain company, and (c) first-person plural pronouns as an inclusive pronoun as in "before we proceed further" which shows that the scammer used "we" to include the target. This shows that scammers, depending on the function of their pronouns, can be personal, exclusive, and

inclusive in their conversations with their targets.

Noncommittal. In deception, noncommittal language use is observed when the deceiver lacks commitment to their statements (Dou et al., 2017), as shown in the scammer's constant change of pronouns, as shown in Figure 15.

Figure 15

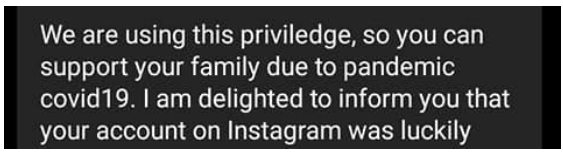
Noncommittal Pronoun Usage

This pronoun usage involves the scammer's initial use of both first-person singular (me, I) and third-person plural pronouns (they, them), which shows that the scammer took ownership of their own actions but also dissociated oneself from the deception by referring to a certain group as the source of their "compensation." However, the succeeding utterances show the scammer's use of first-person plural pronouns (our, we) as in "our dear winner" and "we are not here to play prank with anyone else," which shows that from being a beneficiary of the organization, the scammer has now become part of the group. This pronoun shift in both person and number indicates the scammer's lack of commitment to their pronoun usage and implies ambiguity in their involvement in the scam.

Personal and Exclusive. This is characterized by using first-person singular pronouns combined with first-person plural pronouns that indicate the scammer's shared possession with or membership to a certain group, company, or organization, which makes it exclusive, as shown in Figure 16.

Figure 16

Personal and Exclusive Pronoun Usage



The scammer used the first-person plural pronoun "we," as in "We are using this privilege" to indicate being part of the "giveaway management." However, the use of such plural pronoun shifted to singular as the scammer stated, "I am delighted to inform you," to express the personal sentiments

DOI: https://doi.org/10.53899/spjrd.v29i1.287

of the scammer. Personal and exclusive pronouns represent both the individuality and collectiveness of the scammer's actions.

Impersonal. This involves using first-person singular pronouns and third-person singular pronouns, which suggests an impersonal pronoun usage, as shown below:

Figure 17

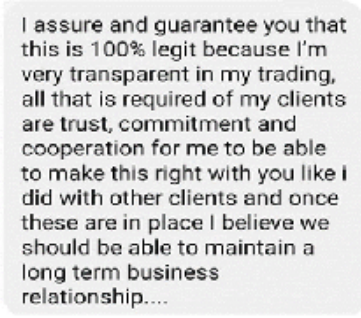
Impersonal Pronoun Usage

As the scammer stated, "This is trade I invested with [name of person] and she help me earned," this suggests that the scammer takes ownership of some actions but also refers to a third party, which may imply that the scammer is either collaborating with another person or distancing one's current account from the scam. Swol and Braun (2014) state that other-oriented pronouns are used in deception to protect oneself, divert attention, and reduce involvement in the action.

Personal and Inclusive. This involves using first-person singular pronouns and first-person plural pronouns as inclusive pronouns to include the target.

Figure 18

Personal and Inclusive Pronoun Usage

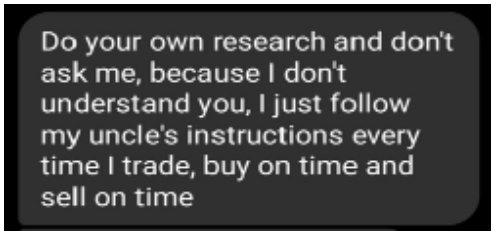


In this example, the scammer used pronouns such as "I believe" to indicate their personal belief and "we should be able to maintain a long-term business relationship" to refer to themselves and the target. Since business transactions are persuasive, using inclusive pronouns signals the scammer's attempt to establish rapport with their target.

Highly Personal. This strategy uses highly personal pronoun usage as the scammer only utilizes first-person singular pronouns throughout the conversation.

Figure 19

Highly Personal Pronoun Usage

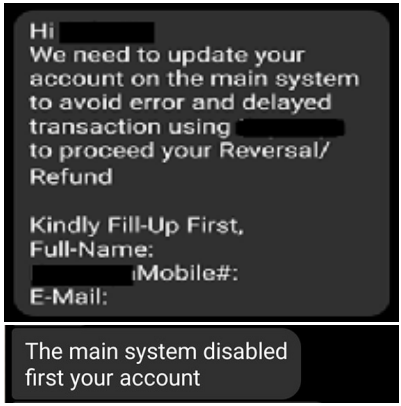


Pronouns such as "I trade" and "don't ask me" were used to refer to oneself. In other words, no other plural pronouns or third-person pronouns were used in the interaction. This signifies the scammer's sole ownership of the actions or thoughts in their utterances.

Ambiguous. Ambiguous pronoun usage is characterized by using pronouns that do not have a clear antecedent or noun reference.

Figure 20

Ambiguous Pronoun Usage



The scammer's use of the pronoun "we" as in "we need to update your account" in their first utterance is considered ambiguous since it may have different interpretations: (1) to indicate the scammer's membership to a certain organization and their need to update the target's account, or (2) to indicate both the scammer's and the target's need to update the account collaboratively. Interestingly, since this is the only pronoun used in the entire conversation, this was replaced in the succeeding utterances by "system" or "the main system." By doing this, the scammer totally distanced oneself from the action and instead put accountability on a nonhuman entity.

DOI: https://doi.org/10.53899/spjrd.v29i1.287

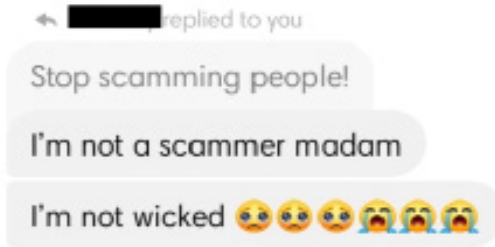
Negation as Linguistic Markers Used by Scammers

According to Roitman (2017) and Horn (2010), negation has many different functions, such as expressing non-existence or absence, rejection or refusal (Roitman, 2017), and denial (Roitman, 2017; Horn, 2010). These were all seen in the research corpus, including other emerging findings on the scammers' use of negation.

Denial. Scammers commonly use this to deny a statement, usually an allegation or expression of doubt made by the target.

Figure 21

Negation Expressing Denial



For instance, the scammer used negation in statements, "I'm not a scammer madam, I'm not wicked," "no scam here," and "this is not a scam" to deny their targets' accusations.

Non-existence. Scammers frequently use this to indicate something is absent or non-existent in the transaction.

Figure 22

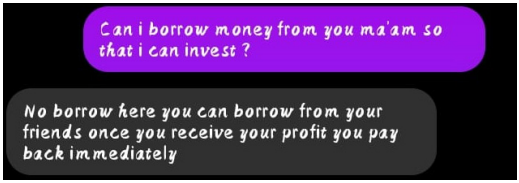
Negation Expressing Non-existence

Scammers use expressions like "no experience is needed," "there will be no access to us," and "No bad content" to indicate the absence of something and emphasize the positive side of their offer.

Refusal. This is done by refusing to accept or grant the target's request. Targets usually make such requests to seek assurance or clarify something.

Figure 23

Negation Expressing Refusal

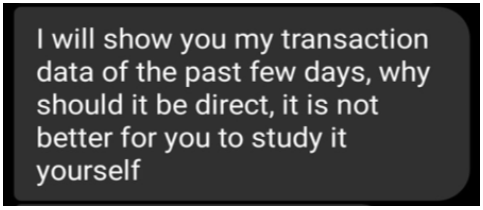


However, scammers use negation, as in "no borrow here" and "There is no call allowed, madam," to turn down the appeal of their targets.

Discouragement. Some scammers use negation to discourage the target from doing or continuing a particular action.

Figure 24

Negation Expressing Discouragement

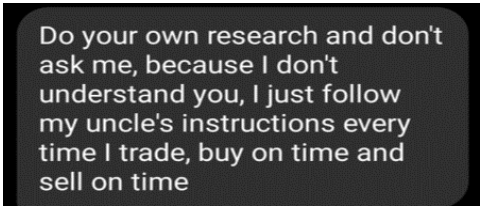


These are seen in expressions like "don't worry about it" and "Don't earn madam" to discourage the target from feeling worried and earning from the offer.

Inability. This is used to refer to the inability of either the scammer or the target.

Figure 25

Negation Expressing Inability

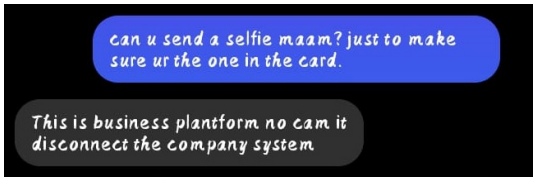


For instance, the negation "don't" in "because I don't understand you" refers to the scammer's inability to understand the target, while the negation "can't" in "If you can't wait to withdraw your profit" refers to the target's inability.

Loss. A few scammers use negation to present a possible loss as a consequence of the target's action.

Figure 26

Negation Expressing Loss

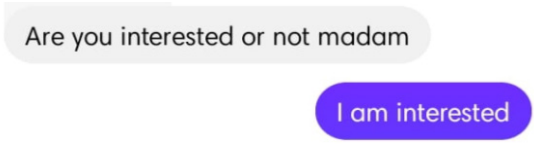


Certain verbs with negative affixes, such as "disconnect" and "disable," are used to refer to the target's possible loss of connection or ability to access one's account.

Contrast. Scammers use negation to present opposing choices.

Figure 27

Negation Expressing Contrast

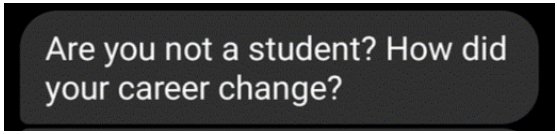


The negation in "Do you want to invest or not, madam?" and "You want to continue or not?" is used by scammers to present contrasting choices to their targets.

Clarification. Clarification is done when there is confusion, and the scammer either presents a clarification or asks for a clarification.

Figure 28

Negation Expressing Clarification

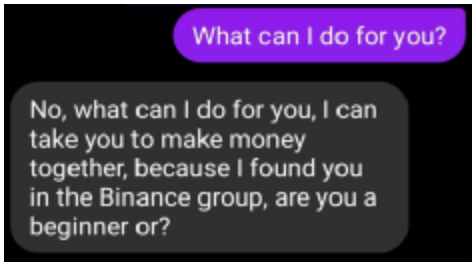


The utterances, "Are you not a student?" and "Aren't you going to study?" both used negation to clarify something from the other interlocutor.

Correction. One scammer used negation to correct the target's assumption.

Figure 29

Negation Expressing Correction



When the target asked the scammer about what they could do for the latter, the scammer replied with, "No, what can I do for you," which involved a negation and a repetition of the target's utterance to indicate a correction on the target's statement.

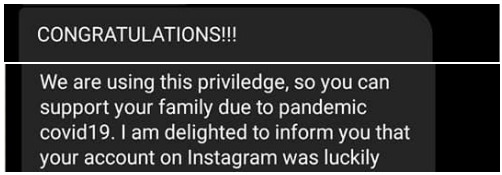
Emotion Words as Linguistic Markers Used by Scammers

The research corpus revealed that the most common emotion words used by scammers are those that express positive emotions. However, various authors stated that negative emotion words are common in deceptive accounts (Dou et al., 2017; Choudhury, 2014; Picornell, 2013). Both these positive and negative emotion words are used by online scammers, as discussed in the following research findings.

Happiness, Astonishment, or Amusement. The most common emotion words scammers use express happiness, astonishment, or amusement.

Figure 30

Happiness, Astonishment, or Amusement



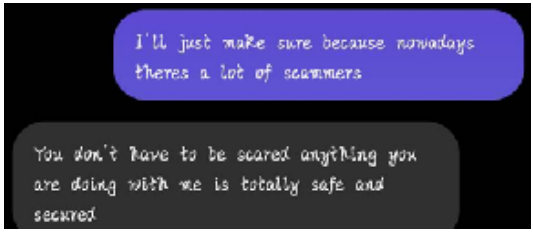
For instance, "CONGRATULATIONS!!!" and "I am delighted" indicate that one is delivering some good news. Additionally, internet expressions, such as "lol" or "lolz" (which means "laugh/laughing out loud" and is usually accompanied by a laughing emoji) and "Hehehehehehe," are used to express amusement in response to scam accusations.

Worry, Doubt, or Fear. Scammers use emotion words that express worry, doubt, or fear to describe the emotions of their targets or other customers.

DOI: https://doi.org/10.53899/spjrd.v29i1.287

Figure 31

Worry, Doubt, or Fear

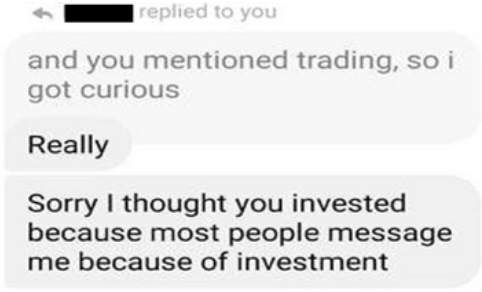


When describing the emotions of others, scammers would use it to promote themselves, as in, "And they are afraid of her, so they come to me and ask me." When the target feels such emotions, these scammers point it out and recommend against it using negation, as in "You don't have to be scared" and "Don't worry about it."

Shame, Regret, or Inadequacy. Scammers use emotion words that suggest their own shame over something that they recognize to be a mistake.

Figure 32

Shame, Regret, or Inadequacy

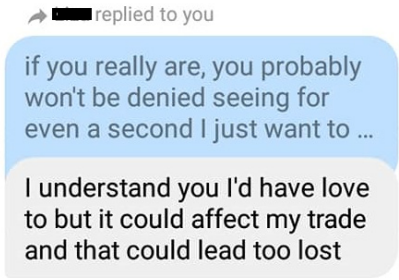


The expression "Sorry, I thought you invested because most people message me because of investment" expresses shame over a misunderstanding, while regret is something that they wish to avoid in their targets, as in "you will not regret doing business with me." On the other hand, the feeling of inadequacy is implied when they apologize for their inability to deal with a particular situation, as stated in their utterances, "Sorry, I can't do that" and "Sorry, I can't send that" that is expressed to refuse the target's request.

Fondness. Scammers use emotion words that suggest desire to indicate their love or fondness towards a certain idea.

Figure 33

Fondness



The utterance "I'd have love to, but it could affect my trade" expresses the scammer's desire. However, in the utterance, "Who would love to go to jail," the word "love" and its sentence construction imply a negation to emphasize that nobody wants to go to jail. This means that such emotion word was used to emphasize either the opposite of fondness or appreciation towards something.

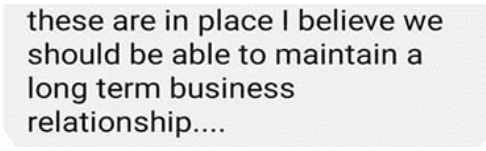
Cognitive Verbs as Linguistic Markers Used by Scammers

The study revealed that scammers use cognitive verbs that indicate equivocation (Merzah & Abbas, 2020; Choudhury, 2014) and express one's knowledge or understanding.

Equivocation. Equivocation is using ambiguous language to conceal the truth or avoid committing to a statement. The cognitive verbs "believe" and "think" are used in deceptive accounts to express the liar's belief (Sandoval et al., 2015; Choudhury, 2014).

Figure 34

Equivocation



These verbs are followed by what the scammer accepts to be true or wants the target to accept as true, as in "I believe we should be able to maintain a long-term business relationship" and "I think you should contact the claiming agent." However, since the use of these verbs equivocates the speaker's statement (Choudhury, 2014; Picornell, 2013), it only suggests one's opinion and implies a lack of certainty or guarantee of the truth.

Expression of Knowledge or Understanding. Cognitive verbs like "know" and "understand" are used by scammers to indicate their knowledge and understanding (or lack thereof). For instance, the utterance "understand what you are saying and it's a normal human to have doubt" expresses the scammer's understanding of the target's doubts.

Figure 35

Expression of Knowledge or Understanding

On the other hand, it is also used with negation, as in "sir, I don't know" and "I still don't understand why you always doubt your chances of success," which expresses the scammer's lack of knowledge and understanding.

Social Actions of Online Scammers and Their Targets

The findings of the study revealed the social actions of the scammers and their targets in their conversations. These actions were categorized into sequences called the pre-offer, offer, insert, and post-offer. All conversations resulted in the rejection of the offer, which is considered a dispreferred response.

Table 3

Social Actions of Online Scammers and Their Targets

Sequence	Sequence-Initiating Action	Sequence-Responding Action	*f*	%	Sample Excerpt
Pre-offer	Asking about the business details (Target's Action as Initiator)	Asking about the target's details (Scammer's Action)	3	37.5	T – "can I ask for more details?" S – "So where are you from"
	Asking about the target's details/ Presenting initial business details (Scammer's Action as Initiator)	Providing one's details (Target's Action)	3	37.5	S – "Firstly I will like to know your name and country eligibility…" T – "Hello good evening Im [name of target] from Philippines"
	Presenting initial business details (Scammer's Action as Initiator)	Asking about more business details (Target's Action)	2	25.0	S – "I hope you will be interested in earning massively from [name of trade] trade?" T – "How it will be earned maam?"
Total			**8**		

Sequence	Sequence-Initiating Action	Sequence-Responding Action	*f*	%	Sample Excerpt
Pre-offer and Insert Sequences	Expressing doubt (Target's Action)	Explaining (Scammer's Action)	68	37.0	T – "I want VCall to make sure… Can I borrow your time even for a second just to see you? S – "…I've so many investors who am also attending too you calling me I'll disturb my signal and loss contact with them"
	Asking about the business details (Target's Action)	Providing business details (Scammer's Action)	62	33.7	T – "How?" S – "You'll have to go to 7/11 for the reference number activation process"
	Asking about the target's details (Scammer's Action)	Providing one's details (Target's Action)	36	19.6	S – "Send your Gcash account. Your name. Your phone number" T – "Name: [Lotlot] Number: [09XXX]"
	Asking about the scammer's details (Target's Action)	Providing one's details (Scammer's Action)	18	9.8	T – "ok, how much did you trade?" S – "10,700 pesos And I paid her commission and withdraw"
Total			**184**		
Offer	Offering money (Scammer's Action)	Rejecting by: a. exposing scam b. withdrawing participation c. indicating implausibility (Target's Action)	5	50.0	S – ""The minimum here is 100$ which is 5k pesos then at the end of Tomorrow which is currently 9pm you withdraw 51k to your Gcash madam" T – "IT'S A PRAAAAAAANK!!! Scammers! Stop scamming people!"
	Providing instructions/ information (Scammer's Action)	Rejecting by exposing scam/ withdrawing participation (Target's Action)	3	30.0	S – "Hello Admin !!!!! Are you interested in posting articles on your page through instant Facebook articles? You will be paid 10 $ per item and every day……/ …… …… Sir, are you interested?" T – "okay no problem im posting you in facebook good day"
	Asking about private information for money/ service (Scammer's Action)	Rejecting by exposing scam (Target's Action)	2	20.0	S – "To update your account what is the latest 6-digit code you received?" T – "According to my friend in NBI its not necessary. My screenshot is enough. Nasaan kna scammer?"
Total			**10**		

DOI: https://doi.org/10.53899/spjrd.v29i1.287

Sequence	Sequence-Initiating Action	Sequence-Responding Action	*f*	%	Sample Excerpt
Post-offer	Insisting by: a. Explaining legitimacy b. Denying scam and questioning (Scammer's	Responding to insistence by: a. Insulting or mocking b. Ignoring (Target's Action)	4	50.0	S – "THIS IS REAL AND LEGITIMATE" T – "[sends a like emoji] Password HULIKABALBON"
	Showing aggression by: a. Insulting (then blocking) b. Asking for explanation (then blocking) (Scammer's Action)	Responding with aggression by: a. Retaliating (then blocking) b. Threatening (Target's Action)	3	37.5	S – "You're a fool" T – "you call me a fool..when you don't even know what is LTT? lol..i am always taught by my school [blocks the scammer]"
	Conceding (Scammer's Action)	Interrogating (Target's Action)	1	12.5	S – "Yeah" T – "how about today"
Total			**8**		

Pre-offer

Based on the online conversations analyzed, either the scammer or the target initiates the pre-offer. This pre-offer refers to the preliminary utterances (Fpre and Spre) introducing the transaction. It is used to project the incoming base FPP and is typically done to avoid dispreference in the SPP (Picornell, 2012).

Fpre → Asking about the business details (Target's Action as Initiator)
Spre → Asking about the target's details (Scammer's Action)

Targets commonly initiated the conversation, usually in reference to a post or someone who mentioned the scammer's profile. In doing so, they inquire about the business.

Figure 36

Asking about business details and asking about target's details

The target started by asking for more business details but was responded by the scammer with, "So where are you from?"—a response that does not answer the question but instead takes the floor by initiating an action through another question.

Fpre → Asking about the target's details/ Presenting initial business details (Scammer's Action as Initiator)
Spre → Providing one's details (Target's Action)

Some scammers initiated the conversation by asking about the targets' details (e.g., name, country) or by presenting the initial business details (info on lottery winnings and instructions in claiming), which were all responded to by their respective targets by providing their own details. These responses signal cooperation, which may urge the scammer to pursue the believing target.

Fpre → Presenting initial business details (Scammer's Action as Initiator)
Spre → Asking about more business details (Target's Action)

Some scammers initiate the conversation by presenting initial business details, such as, "I saw your name on the PBJ list. Have you also heard from them yet?" The target responded by asking another question, "What is PBJ po?" to discuss the business further.

Pre-Offer and Insert Sequences

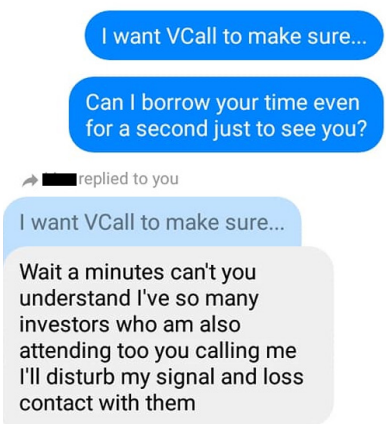
The other pre-offer and insert sequences consisted of probing actions. In particular, probing is present in both the pre-offer sequences (Fpre and Spre) and insert sequences (Fins and Sins) found after the base FPP and before the base SPP. These utterances were found either in the pre-offer, the insert sequences, or, in many instances, both.

Fpre / Fins → Expressing doubt (Target's Action)
Spre / Sins → Explaining (Scammer's Action)

The most common pair that involves probing is when the target expresses their doubt, which is responded to by the scammer's explanation to eliminate the target's suspicion.

Figure 37

Expressing doubt and explaining



DOI: https://doi.org/10.53899/spjrd.v29i1.287

For instance, when the target expressed doubt by asking for a "Vcall" or a video call to "make sure" and "see" the scammer, the scammer refused by explaining that calling would "disturb" the scammer's signal, which would cause loss of contact with the other "investors."

Fpre / Fins → Asking about more business details (Target's Action)
Spre / Sins → Providing more business details (Scammer's Action)

Targets typically ask more questions about the business. In one conversation, the target asked a question about the monitoring procedure, which was responded to by the scammer with a link to a platform that the scammer claimed to be his/her company.

Fpre / Fins → Asking about the target's details (Scammer's Action)
Spre / Sins → Providing one's details (Target's Action)

Scammers acquire information by asking about their targets' personal details since scammers may use such information before presenting the offer. For instance, when the scammer told the target to provide their information (i.e., name and email), the target responded by providing such personal details.

Fpre / Fins → Asking about the scammer's details (Target's Action)
Spre / Sins → Providing one's details (Scammer's Action)

Targets asked questions about the scammers' details. In one conversation about trading, the target asked the scammer how much the latter had traded. The scammer responded to this with the exact amount of "10,700 pesos" and furthered their response by explaining that the latter paid "commission" to the third party. Such questions were asked to help the target decide to trust the scammer and continue the transaction.

Offer

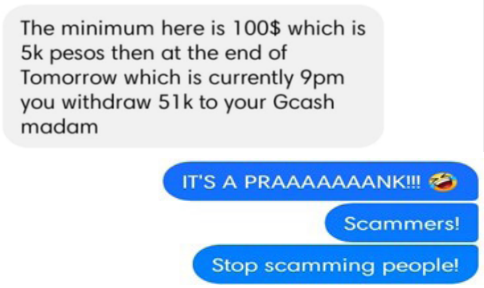
The offer sequence contains the base pair—a pair of utterances composed of the sequence-initiating action (first pair part or FPP) and sequence-responding action (second pair part or SPP) that presents the scammer's actual offer and the target's final response to the offer. After initiating the conversation and probing the details, scammers present their offer. This section presents only the scammer's actual offer (base FPP or Fb) and the target's final response to the offer (base SPP or Sb). In identifying the offer, each conversation was examined to determine the utterance that contains a certain deal (i.e., offering money or information) in exchange for something (i.e., payment or private information) from the target.

Fb → Offering money (Scammer's Action)
Sb → Rejecting by a) exposing scam, b) withdrawing participation, or c) indicating implausibility (Target's Action)

The most common way of presenting an offer is by presenting an offer, which is typically responded to by rejection and done in various ways.

Figure 38

Offering money and rejecting by exposing scam



The offer was presented as a declarative statement that indicates the payment needed (i.e., "100$, which is 5k pesos"). This was followed by insert sequences that involved asking about more details, comparing the business to an alleged Ponzi scheme, and expressing doubt. In the base SPP, the target exposed the "prank" with a laughing emoji and advised scammers to stop. This involves dispreference since it suggested the rejection of the offer and showed a lack of support towards the turn design as it did not contain details responding to the offer. Particularly, this dispreference featured intensification as it strengthened the rejection of the offer through accusation and rebuke.

In another conversation, the monetary offer was responded with "I'm sorry I'm not able to send you money for now I reached the cutoff," which features positioning involving an anticipatory account or apology (i.e., "I'm sorry"), followed by the actual rejection (i.e., I'm not able to send you money for now") and an elaboration or excuse (i.e., "I reached the cutoff"). Lastly, another conversation also involved dispreference by indicating the implausibility of the offer as in "how can 5500 become 30k in days..its like too impossible," which means that the target questioned the legitimacy of the business and implied the rejection of the offer.

Fb → Providing instructions/information (Scammer's Action)
Sb → Rejecting by exposing scam/ withdrawing participation (Target's Action)

Some scammers provide instructions or information that the target can use to earn money, but the exposure of the scam or withdrawal of participation rejects this. For instance, one scammer directly offered by asking about the target's interest in posting articles and explaining the payment. The insert sequences involved asking about the transaction, asking for proof, and expressing doubt. Since the base FPP ended with the polarity question "are you interested," the expected answer is a yes or no, but this turn design was not supported the target said, "okay no problem im posting you in facebook good day" which suggested acceptance and threat. This means that the response featured dispreference, which involved intensification as the threat of "posting" or exposing the scammer online increased the face-threatening nature of the dispreference.

Another offer also involved instructions on what the target should do to "make money," which was immediately rejected by the target. This directness of such dispreference may be attributed to the scammer's inconsistencies in the pre-sequences, which made the interaction confusing for the target. Although the SPP was direct, the response still characterized dispreference as it featured positioning involving a laugh (i.e., AHHAHHAAH) and an apology (i.e., "sorry"), followed by the conjunction "but" and an account explaining the rejection (i.e., "I don't easily trust people I really don't know in personal.").

Fb → Asking about private information (Scammer's Action)
Sb → Rejecting by exposing scam (Target's Action)

The least common way of presenting the offer was by asking about the target's information in exchange for money or service. In one conversation, the scammer directly offered by asking about the target's details to "avoid error and delayed transaction" and proceed with a "refund" via mobile wallet. The FPP ended with an interrogative sentence, "what is the latest 6-digit code you received" and the insert sequences involved asking about the necessity to provide one's personal information. The target's SPP mentioned a third party (i.e., the target's "friend in NBI") and eventually mocked the scammer. In particular, the dispreferred response featured both elaboration (on five different chats of why the target will not provide one's password) and intensification (involving mocks and threats).

Post-offer

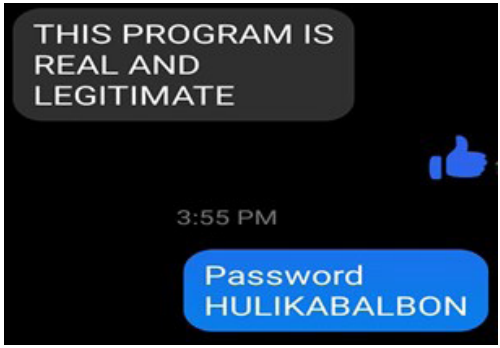
The post-offer presents the exchange of utterances as interlocutors terminate the conversation after the target rejects the offer (base SPP).

Fpost → Insisting by a) explaining legitimacy, or b) denying scam and questioning (Scammer's Action)
Spost → Responding to insistence by a) insulting or mocking, or b) ignoring (Target's Action)

When targets reject the offer, scammers try to remedy this by insisting on the legitimacy of their offer or denying the scam. In response, targets usually point out the scam and insult the scammer or ignore their insistence.

Figure 39

Insisting legitimacy and insulting or mocking



The post-offer features a disagreement with the SPP "Have yourself a legit job" by insisting on the legitimacy of the program (i.e., "THIS PROGRAM IS REAL AND LEGITIMATE"). This was responded to by the target with a like emoji and a mocking utterance (i.e., "HULIKABALBON [You've been caught, hairy person]"). Although the term "balbon" is used to describe someone hairy, the statement "HULIKABALBON" or "huli ka balbon" is used as a Filipino expression to ridicule or make fun of others, which makes the post-offer aggressive.

In another conversation, the scammer denied the allegation and questioned the target. This was observed as a post-offer, where the scammer responded to the target's accusation with amusement as

expressed in "Lol," denial as stated in "I'm not a scammer madam," and a question "Did I scam you?" However, no response was given, meaning the target ignored the scammer's denial and questions.

Fpost → Showing aggression by (a) insulting and blocking, or (b) asking for an explanation and blocking (Scammer's Action)
Spost → Responding with aggression by (a) retaliating (then blocking), or (b) threatening (Target's Action)

In this post-offer, the scammer took the rejection negatively by mocking the target, who responded with retaliation. This comes with blocking, which is done by either the scammer or the target after an exchange of insults. For instance, one scammer called the target "a fool," which was responded to by the target's retaliation and emphasis on one's intellect and was followed by blocking.

In another conversation, the scammer asked the target, "why the sudden change of mind if I may ask," which was responded by the target with a lengthy explanation exposing the scam that involves threats. This was followed by blocking, which suggested the interaction was purposely terminated.

Fpost → Conceding (Scammer's Action)
Spost → Interrogating (Target's Action)

In this post-offer, the scammer shows immediate agreement with the target's rejection by conceding or accepting the scammer's mistake or discrepancy that the target has pointed out. The scammer's one-word agreement (i.e., "yeah") brought closure to the interaction since it was designed to agree with the target's dispreferred response and avoid further talk. When the target expanded the talk by asking, it was turned down by the scammer, who again yielded in persuading the target. The target responded with the typical "oh," which signaled the acceptance of the information. Finally, the scammer responded with a like emoji and another agreement "yeah" to close the conversation.

Conclusion

Online scammers employ different strategies to persuade their targets. They commonly and initially appeal to their targets' positive and negative emotions to persuade them to accept the offer. However, since emotional appeal is insufficient in convincing their targets, scammers also enhance their credibility and use logic to further their persuasion. Despite using varied and multiple strategies, all of the scams in the research corpus resulted in the rejection of the offer, which shows that the quantity of the scammers' strategies did not match the quality of their persuasion.

The deceptive language of the scammers reveals the linguistic choices they made in their attempt to deceive their targets. The scammers' choice and usage of pronouns show how they own their actions, connect to their targets, and dissociate themselves from the transaction. Negation was also common in their utterances and was used to express various things intended to cover the scam.

Additionally, emotion words were observed in some utterances to describe the positive emotions that the scammers and targets wish to have and the negative emotions they wish to avoid. Meanwhile, a few cognitive verbs were observed in the research corpus, and they were used to equivocate the scammers' statements and express their knowledge and understanding (or lack thereof). The analysis of their language contributes to understanding the deceptive persona that the scammers curate online as they interact with their targets.

Moreover, identifying the social actions of the scammers and the targets has reinforced the notion that conversations, as they naturally occur, are indeed a complex process. Interlocutors

DOI: https://doi.org/10.53899/spjrd.v29i1.287

typically engage in several exchanges of utterances and actions before the actual response is given. More importantly, although a dispreference or a dispreferred response is face-threatening and unsupportive of social solidarity, it is advantageous and necessary in certain situations, especially in response to scams.

This research may be used to understand deceptive language and further explore such an understudied phenomenon. However, this study is only limited to the context of failed scams involving Filipino speakers and the analysis of particular linguistic markers. In order to widen our perspective on this subject, it is recommended that successful scams be studied in order to examine the effective use of persuasion in deception, and other markers (e.g., use of all caps and misspellings) be analyzed to investigate such common features in scams. This paper sheds light on the linguistic analysis of deception and contributes to addressing online scams and creating a safer space for virtual communications.

References

Bal, D. & Stone, M. (2021). *Ambiguous pronoun*. Study. https://tinyurl.com/2z5u7vzd

Beebe, S. A., & Beebe, S. J. (2012). *Public speaking: An audience-centered approach* (8th ed). Pearson Education, Inc.

Chiang, E. & Grant, T. (2018). Deceptive identity performance: Offender moves and multiple identities in online child abuse conversations. Oxford Academic. *Applied Linguistics*, *40*(4), 675-698. https://doi.org/10.1093/applin/amy007

Choudhury, F. (2014). Can language be useful in detecting deception? The linguistic markers of deception in the Jodi Arias interview. *Diffusion: The UCLan Journal of Undergraduate Research*, *7*(2),78-92. https://tinyurl.com/mr2z6t77

Dou, J., Liu, M., Muneer, H., & Schlussel, A. (2017). What words do we use to lie?: Word choice in deceptive messages. Cornell University. https://doi.org/10.48550/arXiv.1710.00273

Drew, P. (2013). Conversation analysis and social action. *Journal of Foreign Languages*, *37*(3), 2-20. https://tinyurl.com/3ec4rr44

Giles, D. C., Stommel, W., Paulus, T. M., Lester, J.N., & Reed, D. (2015). Microanalysis of online data: The methodological development of digital CA. *Discourse Context Media*, *7*, 45-51. https://doi.org/10.1016/j.dcm.2014.12.002

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*, *45*, 1-23. https://doi.org/10.1080/01638530701739181

Handoko, H., Putri, D. A. W., Sastra, G., & Revita, I. (2015). The language of social engineering: From persuasion to deception. Andalas University. *2nd International Seminar on Lingustics*, 136-142. https://tinyurl.com/3x6v3xp3

Horn, L. R. (2010). The expression of negation. *Language Arts and Disciplines*. https://doi.org/10.1515/9783110219302

Kapelke-Dale, R. (2021, July 7). Identifying and fixing ambiguous pronouns on the ACT. *Magoosh ACT*. https://tinyurl.com/yc5rxj4a

Lester, J. N., & O'Reilly, M. (2019). Applied conversation analysis: Social interaction in institutional settings. Sage. https://dx.doi.org/10.4135/9781071802663

Maxwell, J. A. (2021). Why qualitative methods are necessary for generalization. *Qualitative Psychology*, *8*(1), 111-118. https://doi.org/10.1037/qup0000173

Meibauer, J. (2018). The linguistics of lying. *Annual Review of Linguistics*, *4*, 357-375. https://doi.org/10.1146/annurev-linguistics011817-045634

Meredith, J., & Potter, J. (2014). Conversation analysis and electronic interactions: Methodological, analytic and technological considerations. *Innovative Methods and Technologies for Electronic Discourse Analysis*, 370-393. https://doi.org/10.4018/978-1-4666-4426-7.ch017

Merzah, S. K., & Abbas, N. F. (2020). Deception in Flynn's psychological thriller Gone Girl (2012): A pragma-stylistic analysis. *European Journal of Literature, Language and Linguistics Studies*, *3*(4), 87-117. https://doi.org/10.5281/zenodo.3766515

Newman, M. L., Pennebaker, J. W., Berry, D. S., & Richards, J. M. (2003). Lying words: Predicting deception from linguistic styles. P*ersonality and Social Psychology Bulletin*, *29*, 665-675.

PACER's National Bullying Prevention Center. (2018). *Why do we use "target" vs. "victim" and "child who bullies" vs. "bully".* PACER Center, Inc. https://tinyurl.com/4zmrntmn

Picornell, I. (2012). The rake's progress: Linguistic strategies for deception. Proceedings of IAFL 10th Biennial Conference. *Centre for Forensic Linguistics*, 153-168. https://tinyurl.com/mrb6bzjd

Picornell, I. (2013). Analyzing deception in written witness statements. *Linguistic Evidence in Security, Law & Intelligence*, *1*(1), 41-50. https://doi.org/10.5195/lesli.2013.2

Roitman, M. (2017). *The pragmatics of negation: Negative meanings, uses and discursive functions.* https://doi.org/10.1075/pbns.283

Sandoval, T., Matsumoto, D., Hwang, H., & Skinner, L. (2015). *FBI bulletin: Exploiting verbal markers of deception across ethnic lines.* FBI Bulleting Archives. https://tinyurl.com/2ndf53af

Schaffer, D. (2012). The language of scam spams: Linguistic features of "Nigerian fraud" emails. *Review of General Semantics*, *69*(2), 157-179. https://tinyurl.com/f3u5sca6

Schegloff, E. A. (2007). *Sequence Organization in interaction: A Primer in Conversation Analysis*, *1*. Cambridge University Press. https://doi.org/10.1017/CBO9780511791208

Shaari, A. H., Kamaluddin, M. R., Fauzi, W. F. P., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *Gema Online Journal of Language Studies*, *19*(1), 97-115. https://doi.org/10.17576/gema-2019-1901-06

Swol, L. V., & Braun, M. T. (2014). Communicating deception: Differences in language use, justifications, and questions for lies, omissions, and truths. *Group Decision and Negotiation*, *23*(6), 1343-1367. https://doi.org/10.1007/s10726-013-9373-3