Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims

Azianura Hani Shaari
azianura@ukm.edu.my
Faculty of Social Sciences and Humanities,
Universiti Kebangsaan Malaysia

Mohammad Rahim Kamaluddin
rahimk@ukm.edu.my
Faculty of Social Sciences and Humanities,
Universiti Kebangsaan Malaysia

Wan Fariza Paizi@Fauzi
fariza.fauzi@ukm.edu.my
Faculty of Social Sciences and Humanities,
Universiti Kebangsaan Malaysia

Masnizah Mohd
masnizah.mohd@ukm.edu.my
Faculty of Social Sciences and Humanities,
Universiti Kebangsaan Malaysia

ABSTRACT

The study of online romance scam is still at its infancy in Malaysia, despite the increase in the number of reported cases in this country. This research primarily aims to identify the steps and strategies involved in the online romance scam in Malaysia. Apart from that, it also aims to identify the pattern of deceptive language used in online romance scam in Malaysia through a comprehensive linguistic analysis of actual online conversations between scammers and victims. The empirical investigation of this research focuses on the language strategies used by scammers as a modus operando in deceiving their targets. With the help of the Malaysian Police Department, a database of romance scam cases was gathered and established. From the database, 30 sets of online communication between scammers and 30 Malaysian victims were selected and analysed using content analysis method. One of the aspects involved in data analysis was scammers' linguistic styles and patterns in manipulating their targets. This was analysed using Brown and Levinson Politeness Model as well as Whitty's Scammers Persuasive Techniques Model. The findings indicate a common linguistic pattern and style of conversation used by online scammers in persuading and deceiving their victims.

Keywords: Online romance scam; linguistic analysis; Politeness Model; Content Analysis; deceptive language

INTRODUCTION

The online romance scam is intimidating since it leaves double impacts to the victims. The first impact is the loss of money and the second one would be the loss of a relationship that involves a deep emotional and psychological trauma (Whitty & Buchanan, 2016). They further state that some victims find it difficult to leave the relationship, even when they have been informed that it is not even real (Whitty & Buchanan, 2016).

eISSN: 2550-2131
ISSN: 1675-8021

Asian Pacific Post (2015) recently reported an increase of the romance scam cases in many Asian countries. They outlined several common warning signs of the Internet dating and romance scams such as prompt expressions of love and other romantic feelings, regular requests for money even at an early stage of a relationship, desperate needs of help and financial problems, various claims of emergencies such as a desperate need for a visa, passport, immigration documents, flight tickets or custom documentation and goods-handling procedures (Asian Pacific Post, December 22, 2015).

THE ONLINE DATING ROMANCE SCAM IN MALAYSIA

In Malaysia, the number of cases involving this crime is increasing at an alarming rate. In 2012 alone, the Malaysian Police Department reported a loss of RM32.09 million due to the Internet Romance Scam (Tan, 2014). In May 2014, Utusan Melayu newspaper reported a disheartening situation in this country that calls for an immediate action. Cyber Security Malaysia reported an increase in romance scam cases in Malaysia, from 4,001 cases (in 2012) to 4,485 cases (in 2013). The head executive of Cyber Security Malaysia, Dr. Amirudin Abdul Wahab states that from the year 2011 to 2013, Cyber Security Malaysia had received not less than 740 reports pertaining to the issue. In fact, in July 2014, the TIME magazine reported that Malaysia was regarded as a global hub for Internet scams due to several reasons such as lax student visa regulations and a sophisticated banking system (Campbell, TIME Magazine, July 9, 2014).

Despite the increasing number of cybercrime cases in this country, the study of online dating romance scam is still at its infancy in Malaysia (Tan & David, 2017). According to Whitty (2012), a lot of work have been done on various types of Nigerian Fraud (also known as 419 scams, a reference to the Nigerian penal code established by the Nigerian government to deal with cyber-crimes) such as phishing emails or Nigerian letters but not much has been done on mass marketing fraud scam and this includes the online dating romance scam (Whitty & Buchanan, 2012b). The present research therefore, is designed to investigate the persuasive language strategies used as a modus operandi in the online dating romance scam. Number of studies have been conducted to identify the steps involved in online romance scam, but what makes our study different from the others would be the focus that gives primary attention to the Malaysian victims.

The focus on the local scenario is important in order to make it suitable for future investigations in this country. One of the important aspects is the contextualised persuasive linguistic strategies used by scammers when approaching Malaysian victims. This helps the authorities to design and implement a more strategic crime prevention method and criminal justice system that recognises online conversation as part of the linguictic evidence in court.

STUDIES ON FAKE EMAILS AND ONLINE SCAM

This section discusses some early studies on online frauds and some psychological tricks used by criminals to dupe victims. These studies are found relevant since the framework of online dating romance scam-analysis also lies within the same concept of persuasive strategies. Among the many international and local studies that are found relevant and helpful in designing the present research are Cukier et al. (2007), Carter (2015), Koon and Yoong, (20130, Whitty and Buchanan (2016) as well as Tan and David (2017).

Previous studies on online frauds have indicated some persuasive techniques in convincing and manipulating victims, and how persuasive language skills have influenced people's emotions (Jones, Towse & Race, 2015) and cognitive behaviour (Modic & Lea, 2013). Carter (2015) proposes an anatomy of written scam communication based on her

analysis on 52 envelopes containing letters and brochures made to deceive targets in granting access to their private accounts, personal details and information, as well as money. According to Carter (2015), scammers intentionally acknowledge that potential victims (recipients) will doubt the content of the letter (such as by saying, 'You don't believe it!') just to create the illusion that the recipient is aware of his or her decision-making options. This is followed with message such as 'do whatever you want' (Carter, 2012, p. 4) that appears to allow recipients to choose the consequences of their actions. Among other strategies gathered by Carter (2015) in her analysis are to provoke recipients' concerns using attention-grabbing words or phrases such as 'all her doubts' (to recognise recipients' concern) and the construction of target's subconscious mind and identity to become someone who is suspicions about the letter, while also implicitly sending a message that doubt is a normal and expected response, but harmless (2015). Unlike the characteristics given in most scam awareness-raising literature, the new modus operandi of cyber frauds acknowledge target's doubt by making the impression that targets are in control and are free to decide whether to respond to the message or not.

According Cukier et al. (2007), e-mail fraud usually involves a rich and emotional narrative with elements of language that provoke feelings of greed (for example: a letter written by a woman who inherited a lot of money from her late husband. The writer promised a portion of the inheritance if the recipient is willing to help with the processing procedures. The lure of easy money triggers a person's sense of greed) and guilt (for example: a letter written by a dying cancer patient who is truly repentant for his past wrongdoings. The writer is looking for somebody to help distribute his large inheritance to the charity. The elements of religion and faith develop recipients' trust and feeling of responsibility. Verses from the bible about doing good deeds, for instance, create the feelings of guilt and shame that make the recipients feel obligated to be act nice and respond to the writer).

Among the common modus operandi would be a persuasion technique that triggers strong emotions involving "peripheral cues and mental shortcuts to bypass logical arguments and counterarguments and to trigger acceptance without thinking deeply about the matter" (Cukier et al. 2007, p. 4). The technique also includes a linguistic strategy that provides emotional distraction to interfere with victims' rationalisation and logical thinking. For example, an appeal letter from someone who is dying from cancer or involved in a tragedy such as war or plane crash (Cukier et al., 2007). According to Zuckoff (2005), cyber criminals usually develop empathy and romantic feelings that influence victims and make them believe that they are sharing similar situations, stories or even expectations with scammers.

Cyber criminals also portray empathy and sincere feelings that distract victims from making rational decision and judgement towards the content of emails or online messages. Cukier et al. (2007, p. 5) put forward the following six techniques in their analysis of fraud messages: (1) Authority- People tend to respond to demands or orders made by someone who has more power or authority. (2) Scarcity- People become highly responsive when a product or service that they want exceeds its supply in a market. (3) Liking and similarity- People show positive reactions towards those who share similar values, beliefs or interests. (4) Reciprocation-People feel a strong obligation to return favours, gifts or invitations. (5) Commitment and consistency- People will remain consistent with certain actions or behaviour and keep their commitment when things are recorded in written documents. (6) Social proof- People tend to conform to the cultural norms, behaviours that are common among the members of their society. In other words, people normally follow the social norms by doing what others do.

eISSN: 2550-2131
ISSN: 1675-8021

PREVIOUS STUDIES ON THE ONLINE DATING ROMANCE SCAM

The online romance scam is described as a "specific type of mass marketing fraud involving situations where scammers pretend to initiate a relationship through online networking sites with the intention to defraud their victims of large sum of money" (Whitty, 2012b, p. 14). Scammers normally look for vulnerable, romantic and lonely people who are looking for a companion or relationship as potential victims (Buchanan & Whitty 2014). Scammers will disguise themselves using various fake identities on social networking sites. They normally approach and establish intimate relationship with potential victims using several techniques and strategies that attract victims to become emotionally attached to them. Once the emotional bond and trust are established, scammers will ask for money by giving various reasons such as emergency situations, illnesses or bankruptcy.

In other studies, maintaining solidarity is one of the strategies established at the early stage of a relationship and this is done through several ways. Firstly, the element of credibility (Koon & Yoong, 2013) is portrayed through the expression of concern. Next, scammers will demonstrate concern towards victims' feelings, and this is usually demonstrated by putting the needs of others before his or her (scammer) own (Freiermuth, 2011b).

Establishing trust would be another criterion involved in the strategies of romance scam (Dixon, 2005; Freiermuth, 2011b) and this is followed by the scammer's act of disclosing some of his/her private information to gain immediate trust. The act of self-disclosure (Henderson & Gilding, 2004) involves the sharing of personal details (Benwell and Stokoe, 2006) will create the illusion that scammers are honest people (Higgins and Walker, 2012; Koon & Yoong, 2013) who trust others with their personal information. This act invites immediate reciprocal trust between strangers who are getting to know each other (Carter, 2015).

Finally, the strategy of giving compliments. Compliments develop solidarity, (Burgoon et al., 2011; Stevens & Kristof, 1995) friendship and interest towards each other. Previous studies have indicated how compliments give good first impression, develop positive feelings and encourage positive feedback and responses from hearers (Seiter and Weger, 2010). It also activates trust and therefore increases victims' tendency to respond to messages (Silvia, 2005; Stevens & Kristof, 1995).

The present study, therefore, was designed to achieve the following objectives:

1. To identify the persuasive language strategies used by scammers to manipulate victims.
2. To propose a list of steps and approaches involved in the online dating romance scam in Malaysia

THE SCAMMERS PERSUASIVE TECHNIQUES MODEL

Buchanan and Whitty (2014) forwarded a model known as the Scammers Persuasive Techniques Model. This model contains a chronology of seven steps and strategies involved in the online dating romance scam. The strategies are: (1) Establishing attractive profiles and send friend requests. (2) Developing trust by asking for victims' personal phone number and/or e-mail, sharing personal stories and demonstrating deep interest in different societies, religions and cultures. (3) Establishing a hyper-personal relationship by exchanging personal photographs and intimate text/voice messages. (4) Grooming the victims by manipulating them to focus solely on the emotional aspect of the relationship and cognitively dismiss any non-rewarding information. (5) Asking for a small amount of money by creating stories such

as car accident, illnesses, bankruptcy or other emergency situations. (6) Maintaining the scam by playing a different character such as authority figure, lawyers, and police. (7) Asking for a big amount of money-if victims refuse, scammers will bargain and lower the amount.

BROWN AND LEVINSON POLITENESS MODEL (1987)

Brown and Levinson's (1987) politeness model is a comprehensive framework that describes people's behaviour when communicating with each other. This model is seen as a suitable framework for the present research because it explains common communication strategies that people use when approaching strangers, establishing a new friendship and maintaining existing relationships.

According to them, language model is naturally face-threatening. People normally employ different forms of linguistic strategies just to protect and maintain each other's face. Among the important aspects of this model are positive face, negative face and face threatening act (FTA). Positive face is "the desire of every member of a culture that his/her wants be desirable to at least some others" (Brown & Levinson, 1978, 62). This includes the internal desire to be understood, approved of, liked or admired by others. Positive face also includes the need to be accepted by others and to know that his or her wants are shared by others.

Negative face, on the other hand, is defined as "the desire of every competent adult member of a culture that his/her actions be unimpeded by others" (Brown & Levinson, 1978, p. 62). In other words, a person's negative face is the need to be independent, to have freedom of action, and not to be imposed on by others. In simple terms, negative face is the need to be independent and positive face is the need to be connected.

FTA is an act that threatens the face wants of an interlocutor. FTAs may threaten either the speaker's face or the hearer's face, and they may threaten either their positive face or negative face.

Some of the examples of FTA forwarded by Brown and Levinson (1987, pp. 67-68) are:

The acts that threaten speaker's negative face	The acts that threaten speaker's positive face
Expressing thanks (speaker accepts a debt, humbles his own face).	Apologies (speaker indicates that he regrets doing a prior FTA, thus damaging his own face to some degree).
Acceptance of hearer's apology (speaker may feel constrained to minimize hearer's guilt).	Acceptance of a compliment (speaker may feel constrained to compliment hearer in turn).
Excuses (speaker indicates that he thinks he had a good reason to do something).	Self-humiliation, acting stupid, self-contradicting.
Unwilling promises and offers (speaker commit himself to some future action although he doesn't want to).	Confessions, admissions of guilt or responsibility.

THE STUDY

Content analysis was conducted based on Zhang and Wildemuth's (2009) process of qualitative content analysis that involves the following seven steps: (1) Preparation of data. (2) Defining the units of analysis. (3) Developing categories and coding scheme. (4) Testing coding scheme on a sample of text. (5) Coding all texts. (6) Assessing coding consistency. (7)

Drawing conclusion from the coded data. Several models and previous findings, as mentioned previously were also recognised as part of the framework. To achieve the aim, a set of authentic online communication (online chat) was selected using a purposive sampling technique- sample was selected based on certain characteristics and the objective of the study. The characteristics are: (1) Malaysian citizens (male or female) who have experienced the online dating romance scam. (2) Malaysian victims who have made at least one money transaction to the criminals. (3) Malaysian victims who are willing to share their experience and data (online conversations with scammers) with the researchers.

A set of data was gathered from the following resources:

1. A Facebook page known as Romance Scam Research Malaysia that was established in 2015. This social site acts as a learning platform for the society to get information about online romance scam in Malaysia. Through the page, we also encouraged victims to come forward and share their stories. 50 victims volunteered to share their experiences with the researchers.
2. Apart from that, the present research also received full support from the Commercial Crime Investigation Department (CCID), Royal Malaysia Police. Through the collaboration, 10 victims have agreed to take part in the study and share their experiences and data (the online conversation that they had with scammers).

60 sets of online conversation were gathered. The first stage of content analysis was conducted to identify the general steps and strategies involved in the online dating romance scam before a thorough linguistic analysis was carried out. The analysis was conducted based on:

1. Scammers Persuasive Techniques Model (Buchanan and Whitty 2014)
2. The six techniques of online scam (Cukier et al. 2007). The present study, however, will only focus on linking and similarity as well as commitment and consistency.

This stage is important, not only as a part of the preliminary analysis, but also to fulfill the first four steps of the content analysis (preparation of data, defining the units of analysis, developing categories and coding scheme as well as testing coding scheme on a sample of text). Next, 30 sets of conversation (from 30 victims) were selected (from the same group of samples) to be further analysed. The selection of sample was made based on the following criteria:

1. Victims who had gone through all the stages of online scam. This was identified in the first stage of content analysis, based on the Scammers Persuasive Techniques Model (Buchanan and Whitty 2014).
2. Victims who had made at least one money transaction to scammers.

The linguistic analysis (for content analysis-part 2) was conducted based on Brown and Levinson's (1987) politeness strategy. The findings were also compared with the linguistic strategies of romance scam proposed by previous researchers (Tan & David, 2017; Carter, 2015; Koon & Yoong, 2013; Whitty, 2015; Cukier et al., 2007)

FINDINGS

Discussion of findings is divided into two sections. Part 1 involves an overview of the overall strategies of online romance scam. The next part, (Part II) is the analysis of language use by scammers when approaching and manipulating victims.

eISSN: 2550-2131
ISSN: 1675-8021

CONTENT ANALYSIS-PART 1

The first stage of content analysis involved 60 sets of online chatting between 60 victims and scammers and this was conducted to identify the general strategies of romance scam and to determine the coding schemes for the next stage of analysis. This was done based on the Scammers Persuasive Techniques Model (Buchanan & Whitty, 2014) together with several techniques of online scam forwarded by Cukier et al. (2007).

Our findings, however, indicate a slightly different set of strategies of romance scam as compared to Whitty's model. Based on the findings, some of the strategies given by Buchanan and Whitty (2014) were perceived as overlapping and redundant. The strategies are developing trust and establishing a hyper-personal relationship by exchanging personal photographs and intimate text/voice messages.

The analysis was performed by looking at the overall online conversations between scammers and victims. The purpose of the first analysis was to identify the overall structure and pattern of this crime, based on the conversations between scammers and Malaysian victims. We divided the scammers' strategies into three stages: initial, pre-attraction and hooked.

The first stage involves setting up contact and establishing relationship. At this stage, scammers initiated a relationship and see the tendency of how vulnerable the targets are (as potential victims) whereas targets will also assess scammers' profile, just to see his or her potential to become a partner. The style of communication at this stage was formal and decent. No romantic words or phrases such as 'I like you', 'I love you' or 'You are my type' were found at this stage. The following excerpts demonstrate how scammers introduce themselves to victims:

> Scammer 5:
> *I am a widower, my wife died years ago in a plane crash, I don't want to talk about that now because it hurts me so much anytime I remembers the ugly incident.*
>
> Scammer 18:
> *I am from Hong Kong but i live in New York, United State of America. I was born and grew up here in United State. I am single with a wonderful beautiful daughter. I am a Petroleum and Chemical Engineer. I work in Oil wells, offshore oil rig and i work on contract bases. I am also into oil business. I buy and sell Oil and Chemicals*

The subsequent stages involved more personal level of communication between both parties (scammers and victims). Stage 2 involves the establishment of credibility – scammers portrayed themselves as a good, friendly, romantic, and/ or religious person who is keen to learn more about victim's background, language and culture. The frequency of correspondence will increase, along with the degree of trust. In the final stage, monetary requests will be made using several techniques after targets have completely fallen for scammers. Descriptions of each stage based on the analysis of findings are given as follows:

INITIAL STAGE- STAGE 1:

Strategy #1 is the analysis of criminals' profile. This was performed based on the following information: culture background, profession, education, image, friends/associates). The following general criteria were found based on the analysis of 60 criminal-profiles:

eISSN: 2550-2131
ISSN: 1675-8021

1. The initiator meets the characteristics stated in Strategy #1 (i.e. a professional and European).
2. Fake profile picture-one photo or photos with exaggerated information pf a rich and luxury lifestyle.
3. Friend list- no friends/very small number of friends/only Asian women/men (when he/she claims to be a European).

PRE-ATTRACTION (EARLY TO MIDDLE STAGE OF RELATIONSHIP)- STAGE 2

Scammer will strengthen the relationship. Among the linguistic features that were identified based on the analysis:

1. Words/expressions with religious connotation (present/more if target has religious inclinations) – '*Assalamualaikum*', '*Salam*' and, 'Peace upon you', 'Allah God bless you'
2. Words/phrases that indicate trustworthiness – 'I will be your man, 'Trust me', 'I'm very honest', 'I believe in you'.
3. Words/phrases that express attraction towards the victim – 'all I want', 'I really want', 'You are my type', 'I like you', 'I love you', 'I miss you every day'.
4. Words/phrases that prioritize the victim – 'This is for our future', 'Your daughter is my daughter', 'This is only for you'. 'I have been dreaming for', 'cannot imagine', 'wherever you go', 'through all your days', 'now or never', 'every way', 'all the time', 'so much'.

HOOKED (MIDDLE TO END)-STAGE 3:

At this stage, monetary request was initiated. Sometimes, words expressing gratefulness were employed together with the request. Writing style at this stage was found more aggressive, forceful and sometimes rude. Some common scenarios used by the scammer:

1. Scammers promised to send gifts and then requested immigration tax payment for delivery purposes.
2. Scammers were stranded at the airport/ at the custom/ immigration office.
3. Scammers had financial problems and needed cash immediately.
4. Scammer had an accident and is forced to pay compensation immediately
5. Family members were diagnosed with serious illness

CONTENT ANALYSIS- PART II

Our analysis suggests 16 common steps and strategies used by scammers in deceiving and manipulating victims. These steps and strategies bear resemblance to some common politeness strategies and behaviors given by Brown and Levinson (1987). We divided the overall steps into three main stages. Stage 1 (or initial stage) involves strategies such as setting up contact and establishing relationship. Stage 2 (or pre-attraction stage), involves activities such as gaining trust, developing personal relationship and grooming process whereas stage 3 or what we categorised as hooked involves criminal activities such as maintaining the scam, baiting or luring, as well as the execution of real crime.

The analysis also found some politeness strategies used by scammers to establish relationship with victims before executing scamming activities. The categorisation of politeness strategies, together with sample of conversation are demonstrated in the following table:

TABLE 1. Categorisation of Politeness Strategy and Sample of Conversation

Online Romance Scam-Attack Framework	Description of Acts (or Strategy)	Categorisation of Strategy	Sample of Actual Online Conversation between Scammers and Victims
Stage #1- Initial (*Setting up contact and establishing relationship*) At this stage, a profile check of the initiator will be performed before getting into the relationship.			
Stage 1.1- Setting up contact	Scammer displays interesting fake profile on social media		Scammer 24: *I am Yusof, 42, from Shah Alam, Selangor, Malaysia based in UK, I'm divorced have one kid, a girl of two years. I work as Offshore Manager at Liverpool Bay Oil and Gas Fields, United Kingdom. Would like to know you more if possible, you give your whatsapp or viber number. Thanks, Yusof.*
Stage 1.2- Establishing Relationship	Scammer introduces his background. Some scammers provide interesting stories.		*Sc*ammer 22: *My name is Dasuki currently living in London, i am from Kedah Malaysia, but i was born and brought up in London, I am into real estate management and properties business in London, i am a widower, i lost my wife in car accident, please where are you from?*
Stage #2 –Pre-Attraction *(Gaining trust, developing personal relationship and grooming process)* The process of manipulating the victim to focus on the emotional cues and cognitively dismiss and non-rewarding information.			
Stage 2.1- Gaining Trust	Positive Politeness Strategy 1: Scammer indicates similarities with victim to claim common ground	**Step 1:** Claim common Ground Scammer shows similarities between him and target victim.	Scammer 15: *Assalamualaikum friend. Thanks for accepting my friend request. Is my pleasure to have you.*
Stage 2.2- *Developing Personal Relationship*	Positive Politeness Strategy 2: Acts that indicate association between scammer and victim	**Step 2:** Scammer notices and attend to victim's interests and wants	Scammer 27: *My love…good Morning from the city of Malaysia, am so happy and excited to hear from you, indeed you mean so much to me…*
Stage 2.3- Grooming Process		**Step 3:** Scammer shows concern of victim's needs and wants	Scammer 27: *Honey I hope you are fine. Happy sound and healthy my love. I miss you with my whole heart*

		Step 4: Scammer exaggerates interest/sympathy/ approval/ towards victim	
		Step 5: Scammer strengthens his interest towards the victim (or at least makes victim feels as it is)	Scammer 26: *I want to marry you* *No I'm very serious* *You are my type of woman*
		Step 6: Scammer makes interesting offers	Scammer 26: *Guess what?* *Tuesday is my birthday* *So I shall give some gift to my friends so you as my wife* *What would u like me to give to you?*
		Step 7: Scammer shows the act of togetherness by including victim into his future plan	Scammer 26: *When do you plan of coming to London?* *I want you to come and pay me a visit* *I will pay for your visa*
		Step 8: Scammer urges for reasons or give reasons for his action	Scammer 7: *i just want you to appreciate me and open up your love and heart to me ok* *i am so in love with you* *all i want is for you to be honest to me ok* *you promise to be honest with me darling?*
	Negative FTA Strategy 3: Scammer makes valuable offers. This put pressure on victim to accept or reject the fast-moving relationship. Victim feels obliged to fulfil the request.	**Step 9:** Scammer indicates that he wants victim to commit herself to whether she wants to do something for the scammer.	Scammer 26: *Let me know today because I will be going for shopping* *Once I buy them **tomorrow** I will send it for you to see if you like*
	Positive Politeness Strategy 4: Scammer shows attempt to fulfil victim's wants and needs	**Step 10:** Scammer offers interesting gifts	Scammer 7: *i will include some other great stuff too like perfumes, ladies handbags and a surprise* *brown envelope* *inside the parcel ok* *i am in the shopping mall now*

			is ok dont worry ok
		Step 11: Show sympathy, understanding, cooperation	Scammer 26: *I will put 10000pounds in the package so that you use it to prepare your visa* *you can use the money to buy whatever he needs in school till December* *Because I will come and visit*
Stage #3- Hooked *(Stages- Maintaining the scam, the bait, execution)*			
Strategy 3.1- Maintaining the Scam	**Step 12:** Scammer assumes a different character (authority figure, lawyers, and police) to present a new excuse for the money.		Involvement of other parties such as bank officers or custom officers (No politeness strategies involved)
Strategy 3.2- The bait Test the waters by asking for a gift or some crises such as car accident, family member sick, injured in war, problems in business have occurred.	Negative FTA Strategy 4: Scammer put pressure on victim by asking him/her to do (or refrain from doing) something. These acts (or strategies) prompt drastic responses from victim.	**Step 13:** Orders and request: Scammer indicates that he wants victim to do or avoid from doing something.	Scammer 4: *This is not done yet and as I have emailed him that I am hospitalized and cannot go to the bank.*
Stage 3.3- Execution Scammer asks for money.		**Step 14:** Suggestions and/or advice: Scammer convinces victim to do as he says **Step 15:** Sending reminders: Scammer reminds or indicates that victim should remember to do something **Step 16:** Threats, warnings, dares: Scammer indicates that he will take certain actions if victims refuse to do something.	Scammer 28: *Please honey can you send to me 10,000 USD first thing tomorrow morning?* Scammer 10: *You are involved now. They will find you.*

Some acts in the earliest stages of the relationship were intentionally performed to build rapport and develop friendship and solidarity between strangers. Among the common politeness strategies used by scammers would be to claim common ground, demonstrate similarities and a strong interest (Brown & Levinson, 1987) towards victims.

Scammers 15 and 17, for instance, initiated their conversations with '*Assalamualaikum'* (an Arabic greeting with religious connotation means peace be upon you) when approaching two Muslim victims. Scammer 24 on the other hand, introduced himself as '*Yusof'* from Selangor to a victim, who is also living and working in Selangor. Scammer 18, on the other hand, introduced himself as an offshore manager name Abdullah (on an online social platform that gathers professionals known as LinkedIn). He claimed that he attended one international conference in Kuala Lumpur, Malaysia, fell in love with the city, thus decided to open his LinkedIn account there (the same online platform where he met the victim). Salmon (1996) claimed that sharing common knowledge or certain personal characteristics is important in establishing new reciprocal relationships among people. The use of popular names such as 'Yusof' and 'Abdullah'; one of the most common names in Malaysia with 47,989 registrations in 2017 (Noor Atiqah Sulaiman, New Straits Times, 4 October 2018) is seen as a strategy that helps create common ground and minimize distance between two strangers who are starting a new friendship.

Scammer 22 introduced himself as *'Dasuki*' who were born in Kedah, Malaysia but living and working in London. This strategy (claiming as someone from the same hometown) creates instant connection with the victim who is also living within the same area of the country (the northern part of Malaysia). Dasuki (scammer 22) also introduced himself as a widower. This is one of the strategies since the victim has revealed her status as a single mother on her social media-profile. Scammer 16 repeatedly used the word '*Jannah*' (an Arabic word means heaven or forever) when describing his everlasting love to the Muslim victim. By using familiar names (of people and places) scammers managed to attract victims' attention to establish instant relationship and connection.

Previous studies have indicated the use of religious symbols and persuasive language skills (Bahiyah Abdul Hamid & Amalina Shahdan, 2018) as powerful marketing strategies in businesses. Abou Bakar, Lee and Rungie (2013) for instance, found a significant impact of religious symbols on product packaging and how these symbols increase consumers' intention and interest to purchase products. Global entrepreneurs are aware of the potential persuasiveness of religious words and symbols in advertising. In fact, religious symbols and words not only help gain consumers' trust towards the products, but also enhance people's perceptions of the service-providers' quality and business integrity (Taylor, Halstead & Moal-Ulvoas, 2017). For cyber criminals and scammers who gain profit through various manipulative techniques and strategies, this purported marketing approach is seen as an effective method of earning people's interests, trust or empathy.

Language skills, social adjustment and cultural differences are among the most challenging issues faced speakers of different nationalities (Najeeb et al., 2012). These intercultural communication issues, however, can be minimised using certain politeness strategies that are universally understood and accepted (Marlyna Maros & Liyana Rosli, 2017). Morrow (2017) describes the act of claiming common ground as a cognitive tool that speakers normally use to facilitate conversation. Claiming common ground is seen as a common strategy used by scammers as some early stages of the relationship (stage 1.1 until 2.2) since it helps develop shared knowledge and this relies heavily upon speakers' existing knowledge on victims' social context, cultural values, norms and beliefs (Brown-Schmidt,

2012; Knusten & Le Bigot, 2012). As a result, a smooth communication is achieved when scammers' and victims' knowledge overlaps (Brown-Schmidt, 2012; Knutsen & Le Bigot, 2012). In other words, demonstrating common ground not only helps to achieve consensus between scammers and victims, but also reduce any form of cognitive dissonance between strangers. This leads to the next stage of a relationship that includes emotional acceptance and trust development.

EMOTIONAL ACCEPTANCE AND DEVELOPMENT OF TRUST

The next strategies would be to pay attention and express extra concern to victims' needs and wants. These include victims' need for attention, kindness and approval. This is performed by exaggerating interests and/or sympathy towards the victims (step 2- step 5). This strategy brings instant connection, emotional acceptance and trust, especially among lonely victims (Button, Nicholls and Kerr, 2014). Among the common lexical items used at these stages (based on the frequency of occurrences) are 'hope' (64 occurrences-15 scammers), 'give' (62 occurrences-16 scammers), 'heart' (40 occurrences-16 scammers), 'understand' (32 occurrences- 9 scammers), 'wish' (19 occurrences-8 scammers), 'promise' (18 occurrences-10 scammers) and 'care' (53 occurrences-10 scammers). Other frequently-used words and adjectives to attract victims 'attention would be, 'god' (33 words- 6 scammers), 'bless' (13 occurrences- 5 scammers), 'lovely' (11 occurrences- 5 scammers), 'beautiful' (13 occurrences-6 scammers), 'friends' (28 occurrences- 15 scammers), 'friendship' (13 occurrences- 6 scammers) and 'great' (13 occurrences-11 scammers).

THE ACT OF GIVING COMPLIMENTS

Previous studies have indicated the function of compliments in developing solidarity (Tan & David, 2017; Azianura Hani Shaari, 2017; Carter, 2015; Koon & Yoong 2013; Whitty, 2015; Burgoon et al., 2011; Stevens & Kristof, 1995) that motivate victims to believe that scammers are having the same feelings with as them. Not only that, compliments also stimulate positive feelings that help develop trust, which increases victims' tendency to respond to romantic messages (Silvia, 2005; Stevens & Kristof, 1995). Our analysis found that compliments were given generously in the early stage of the relationship (Stage 1.1-establishing relationship until 2.3-grooming process). Some of the examples are given as follows:

THE FINAL STAGE- EXECUTION

The third and final stage, (termed as execution, demonstrate a change of linguistic behavior among most scammers. This stage is termed as execution due to the following reasons:

1. This is the stage where scammers normally revealed their real intention behind the fake relationships.
2. This is the stage that involves an aggressive request of monetary. Scammers will persuade and force victims to transfer money by sending regular reminders, threats and warnings.
3. At this stage, the use of romantic words, compliments and promises are reduced; and most conversations only focused on personal benefits and money transactions.

At these last few stages, scammers will become more aggressive and be assertive towards victims. Demands will be made in direct manners and scammers will use several linguistic strategies that create a sense of urgency to claim instant money. In Brown and

Levison's Politeness Framework, this strategy is categorised as belonging to the negative politeness strategy. A direct act of claiming something or making requests impedes a person's needs for freedom of action which might create a sense of responsibility (or guilt) to follow the orders.

Among the common lexical items used at these sub-stages are 'tomorrow' (35 occurrences-11 scammers), 'business' (32 occurrences- 9 scammers), 'airport' (29 occurrences- 5 scammers), 'need' (12 occurrences- 6 scammers), 'urgent' (19 occurrences-4 scammers), 'order' (14 occurrences- 6 scammers), 'prepare' (14 occurrences- 4 scammers), and 'serious' (14 occurrences- 7 scammers).

Scammer 4 for instance, claimed that he was hospitalised for several days and needed money for medical bills. He constantly reminded the victim to bank in money for that emergency purposes. Scammer 6 claimed that some of his goods that were sent to Malaysia were held at the custom office, thus money was needed urgently to retrieve the packages. Scammer 27 claimed that something went wrong with his machine thus he needed 10,000 USD to fix the machine as soon as possible. These are among the emergency situations created by scammers to manipulate victims and implement emotional responsibility to provide financial support for their fake lovers.

The analysis of 30 sets of online conversation (between 30 scammers and 30 victims) has led to the following 16 common steps and strategies employed by romance-scammers in manipulating Malaysian victims:

Stage 1: Setting up contact and establish relationship

Stage 2: Gaining trust (claim common ground) and developing personal relationship

i. Step 1: Claim common Ground-Scammer shows similarities between him and target victim.
ii. Step 2: Scammer notices and attend to victim's interests and wants.
iii. Step 3: Scammer shows concern of victim's needs and wants.
iv. Step 4: Scammer exaggerates interest/sympathy/approval/ towards victim.
v. Step 5: Scammer strengthens his interest towards the victim (or at least makes victim feels as it is).
vi. Step 6: Scammer makes interesting offers.
vii. Step 7: Scammer shows the act of togetherness by including victim into his future plan.
viii. Step 8: Scammer urges for reasons or give reasons for his action.
ix. Step 9: Scammer indicates that he wants victim to commit herself to do something him.
x. Step 10: Scammer offers interesting gifts.
xi. Step 11: Both scammer and victim show sympathy, understanding, cooperation towards each other.

Step 12: Scammer assumes a different character (authority figure, lawyers, and police) to present a new excuse for the money.

Stage 3: Maintaining scam, the bait and execution

i. Step 13: Orders and request: Scammer indicates that he wants victim to do or avoid from doing something.
ii. Step 14: Suggestions and/or advice: Scammer convinces victim to do as he says.
iii. Step 15: Sending reminders: Scammer reminds or indicates that victim should remember to do something.
iv. Step 16: Threats, warnings, dares: Scammer indicates that he will take certain actions if victims refuse to do something.

Even though not all conversations adhered to every single step and strategy mentioned it is also important to note that all sets of online chatting between scammers and victims involved in the analysis did not exclude or skip any of the three main stages mentioned, which are establishing relationship, gaining trust, maintaining the scam, as well as the execution of real agenda.

CONCLUSION

In conclusion, the findings of the present research managed to identify some common steps and persuasive language strategies used by scammers in manipulating victims. Some positive politeness strategies such as claim common ground, indication of interest, membership and similarities were found at some early stages of the relationship. However, towards the end of the short relationship, the entire politeness strategy basically shifts from positive to negative and this involves acts such as direct claims, statements, and requests. Before executing the real crime, victims' need for freedom will be maintained and this is done by given choices for victims to fulfil the requests or simply turn down the offers (some scammers begin their scam by offering interesting gifts, cash, business proposal or investment scheme).

Scammers normally become aggressive towards the end of the process. This usually happens when victims have come to their senses and decided to end the relationship. At this stage, however, some transactions could have been performed, or at least half of the payment has been transferred to fake accounts. The present study found some of the strategies suggested by these early researchers such as linking and similarity, commitment and consistency (Cukier et al., 2007) portrayal of credibility (Koon & Yoong, 2013) trust development strategy (Carter, 2015) as well as the act of giving compliments (Tan & David, 2017; Carter, 2015; Koon & Yoong, 2013; Whitty, 2015; Whitty & Buchanan, 2016). Discussion of these approaches, however, were made from the perspectives of politeness strategies that is found very common in human communication (Brown & Levinson, 1987). Based on the analysis, some distinctive strategies of romance scam cases involving Malaysian victims would be:

1. The use of local names for people and places.
2. When scammers created stories and tried to relate themselves with big companies and businesses, they would refer to some famous local brands and the most common one is *Petronas* (8 scammers).
3. Even though most scammers (the main actor who initiated the love-relationship) that were caught by the Malaysian Police Department hold international passports (Azianura Hani Shaari, Yeap Yoke Peng, Mohammad Rahim Kamaluddin, 2018), the crime always involved Malaysian partners who act as custom officers, policemen, and bankers. Conversation between victims and these local accomplices, however, normally takes place over the phone (Stage 12) and is performed in local languages (Malay, Chinese or Tamil language). According to the Malaysian Police Department (Azianura Hani Shaari, Yeap Yoke Peng, Mohammad Rahim Kamaluddin, 2018), the involvement of local partners is important in creating more realistic scenarios and convincing stories. Local accomplices are responsible for gathering victims' information, local documents, registration of local phone numbers as well as local bank accounts for money-transaction. This stage, however, was not thoroughly analysed since it is beyond the scope of the present study. None of the victims involved in the present study kept the recording of the telephone conversation with these third parties.
4. Since Malaysia is a Muslim country, the use of Muslim names and religious phrases is seen as another common strategy. This is particularly different from the findings of

the previous studies (Carter, 2015; Whitty 2015; Whitty & Buchanan, 2016) that laid emphasis on western settings and groups of victims.

The findings of the present research have several implications. Firstly, it is hoped that the findings will help increase the society's awareness on the common persuasive language strategies used by scammers in manipulating victims. Next, it is also hoped that the findings of the present research will contribute to the development of an online application (a web application that detects scam language and gives alert to online users) that helps people to recognize online criminals who toy with people's feelings to gain profit and unnecessary pleasure. It is also hoped that the present research will provide a basis for the development of more future studies pertaining to the same crime in Malaysia such as a correlational research that explores the relationship between an individual's pattern of language, psychological attributes and criminal behavior. Finally, it is also hoped that the findings will help the authorities to combat this crime and reduce the number of romance scam-victims in Malaysia.

ACKNOWLEDGEMENT

This study was made possible from a research grant provided by the Fundamental Research Grant Scheme (FRGS), Ministry of Higher Education Malaysia, **FRGS/1/2016/SS06/UKM/02/2**

REFERENCES

Abou Bakar, Lee, R. & Rungie, C. (2013). The Effects of Religious Symbols in Product Packaging on Muslim Consumer Responses. *Australasian Marketing Journal. Vol. 21*(3), 198-204.

Azianura Hani Shaari. (2017). *Language of the Digital Minds*. Bangi: Penerbit Universiti Kebangsaan Malaysia.

Azianura Hani Shaari, Yeap Yoke Peng & Mohammad Rahim Kamaluddin. (2018). *Jenayah Cinta Siber.* Bangi: Penerbit Universiti Kebangsaan Malaysia.

Bahiyah Abdul Hamid & Amalina Shahdan. (2018). Total Fairness Inside-out: Linguistic Features in Whitening Product Advertisements. In Bahiyah Abdul Hamid, Lee Siew Chin & Azianura Hani Shaari (Eds.) *Discourse in Practice: From Conventional to Digital*. Bangi: Penerbit Universiti Kebangsaan Malaysia.

Benwell, B. & Stokoe, E. (2006). *Discourse and Identity*. Edinburgh: Edinburgh University Press.

Brown, P. & Levinson, S. C. (1987). *Politeness: Some Universals in Language Usage (Vol. 4)*. Cambridge University Press.

Brown, R. & Gilman, A. (1972). The Pronouns of Power and Solidarity. In Sebeok, T. A., (Ed.), *Style in Language* (pp. 253-276). MIT Press.

Burleson, B. R. & Holmstrom, A. J. (2008). Comforting communication. *The International Encyclopaedia of Communication*.

Burgoon, J.K., Guerrero, L.K. & Manusov, V. (2011). *Nonverbal Signals. The SAGE Handbook of Interpersonal Communication*. London: SAGE.

Buchanan, T. & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law. Vol. 20*(3), 261-283.

Brown-Schmidt, S. (2012). Beyond common and privileged: Gradient representations of common ground in real-time language use. *Language and Cognitive Processes. Vol. 27*(1), 62-89.

Button, M., Nicholls, C.M.N. & Kerr, J. (2014). Online frauds: Learning from victims why they fall for these scams, *Australian & New Zealand Journal of Criminology. Vol. 47* (3), 391-408.

Brulliard, K. (2009). Worldwide Slump Makes Nigeria's Online Scammers Work That Much Harder. Retrieved 1st March, 2018 from http://www.washingtonpost.com/wpdyn/content/article/2009/08/06/AR2009080603764.html

Carter, E. (2015). The Anatomy of Written Scam Communications: An Empirical Analysis. *Crime, Media, Culture. Vol. 11*(2), 89-103.

Cukier, W. L., Nesselroth, E. J. & Cody, S. (2007). Genre, Narrative and the "Nigerian Letter" in Electronic Mail. Proceedings of the 40th Hawaii International Conference on System Sciences 2007.

Dixon R. (2005). Nigerian Cyber Scammers. LA Times. Retrieved 15 July, 2017 from http://www.latimes.com/la-fg-scammers20oct20-story

DeBrosse, J. (2008). ID theft victim becomes pawn in dating scam. Retrieved 4 April, 2018 from http://www.daytondailynews.com/n/content/oh/story/news/local/2008/04/06/ddn040608scammers.html

Freiermuth, Mark R. (2011). Text, Lies and Electronic Bait: An Analysis of Email Fraud and the Decisions of the Unsuspecting. *Discourse and Communication. Vol. 5*(2) 123-145.

Goffman, E. (1967). On face-work: An analysis of ritual elements in social interaction. In Jaworski, A. & Coupland, N. (Eds.), 2001. *The Discourse Reader* (pp. 206-320). New York: Routledge.

Holmes, J. (1988). Paying compliments: A sex-preferential politeness strategy. *Journal of Pragmatics. Vol. 12*(4), 445-465.

Higgins, C. & Walker, R. (2012). Egos, Logos and Pathos: Strategies of Persuasion in Social/Environmental Reports. *Accounting Forum. Vol. 36*, 194-208.

Jones, H., Towse, J. & Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations, *International Journal of Cyber Behavior:Psychology and Learning. Vol. 5*(3), 13-29,

Kich, M. (2005). A Rhetorical Analysis of Fund-transfer-scam Solicitations. *Cercles. Vol. 14*, 129-142.

Koon, T. H. & Yoong D. (2013). Preying on lonely hearts: A Systematic Deconstruction of an Internet Romance Scammer's Online Lover Persona. *Journal of Modern Languages. Vol. 23*, 28-40.

Knutsen, D. & Le Bigot, L. (2012). Managing dialogue: How information availability affects collaborative reference production. *Journal of Memory and Language. Vol. 67*(3), 326-341.

Kleinrock, L. (1967). Time-shared systems: A theoretical treatment. *Journal of the ACM (JACM). Vol. 14*(2), 242-261.

Licklider, J. C. R. (1960). Man-computer symbiosis. *IRE Transactions on Human Factors in Electronics. Vol. 1,* 4-11.

Modic D. & Lea SEG. (2013). Scam compliance and the psychology of persuasion, Social Science Research Network. Retrieved 10 October, 2014 from http://dx.doi.org/10.2139/ssrn.2364464

Morrow, K. (2017). Tracking the Common Ground in Dialogues: Cultural and Genre Effects, master's thesis, Department of Linguistics University of Alberta. Retrieved 15 July, 2017 from https://era.library.ualberta.ca/files/cb5644r986/Morrow_Keely_P_201709_MSc.pdf

Najeeb, Zena Moayad, Marlyna Maros & Nor Fariza Mohd Nor. (2012). Politeness in e-mails of Arab students in Malaysia. *GEMA Online® Journal of Language Studies. Vol. 12*(1), 125-145.

Marlyna Maros & Liyana Rosli. (2017). Politeness Strategies in Twitter Updates of Female English Language Studies Malaysian undergraduates. *3L: Language, Linguistics, Literature Vol 23*(1), 132 – 149.

Noor Atiqah Sulaiman. (2018). Naming names: Malaysia's longest, most popular names revealed by NRD. New Straits Times. 4 October.

Rege, A. (20090. What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology. Vol. 3*(2), 494-512.

Salmon, S. J. (1996). Four of a Kind: An Activity to Help Establish Reciprocal Friendships. *LD Forum. Vol. 21*(4), 25-28.

Seiter, J.S. & Weger, Jr, H. (2010). The Effect of Generalized Compliments, Sex of Server, and Size of Dining Party on Tipping Behavior in Restaurants 1. *Journal of Applied Social Psychology. Vol. 40*(1), 1-12.

Silvia, P.J. (2005). Deflecting Reactance: The role of Similarity in Increasing Compliance and Reducing Resistance. *Basic and Applied Social Psychology*. *Vol. 27*, 277–284.

Stevens, C.K. & Kristof, A.L. (1995). Making the Right Impression: A Field Study of Application Impression Management During Job Interviews. *Journal of Applied Psychology. Vol. 80*(5), 587-588.

Schaffer, Deborah (2012). The Language of Scam Spams. Linguistic Features of "Nigerian Fraud" E-mails. *ETC: A Review of General Semantics. Vol. 69*(2), 157-179.

Tan, H. K. & David, Y. (2017). Preying on lonely hearts: A systematic deconstruction of an internet romance scammer's online lover persona. *Journal of Modern Languages. Vol. 23*(1), 28-40.

Taylor, V.A., Halstead, D. & Moal-Ulvoas, G. (2017). Millennial Consumer Responses to Christian Symbols in Advertising: A Replication Study. *Journal of Empirical Generalisations in Marketing Science. Vol. 17*(1).

Whitty, M.T. (2015). Anatomy of the online dating romance scam. *Security Journal. Vol. 28*(4), 443-455.

Whitty, M.T. & Buchanan, T. (2016). The Online Dating Romance Scam: The Psychological Impact on Victims–Both Financial and Non-financial. *Criminology and Criminal Justice. Vol. 16*(2), 176-194.

Wierzbicka, A. (1991). Japanese key words and core cultural values. *Language in Society. Vol. 20*(3), 333-385.

Zuckoff, M. (2005). Annals of Crime: The Perfect Mark. *The New Yorker. Vol. 82*(13), 36-42.

Zhang, Y. & Wildemuth, B.M. (2009). *Qualitative Analysis of Content.* USA: Libraries Unlimited Inc.

ABOUT THE AUTHORS

Azianura Hani Shaari (PhD) is a Senior Lecturer at the Faculty of Social Sciences and Humanities, UKM. Sociolinguistics, culture, gender and identity are among the areas that stay close to her heart. She has received several awards throughout her career and has published many articles in both local and international journals.

Mohammad Rahim Kamaluddin (PhD) has completed his doctoral degree in Criminology and is currently working as a senior lecturer at Human and Societal Well-Being Centre, Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia (UKM). His research interests include criminology, criminal psychology, commercial crimes, crime prevention, victimology, as well as tools and psychometrics.

Fariza Fauzi (PhD) is a Senior Lecturer at the Faculty of Information Science and Technology, UKM. Her research interests include Web information extraction and processing, natural language processing, and cybersecurity. Her work has been published in reputable journals and conferences which include Information Processing and Management, International Journal of Human-Computer Studies and ACM Multimedia.

Masnizah Mohd (PhD) is an Associate Professor at the Faculty of Information Science and Technology, and a member of the Center for Cyber Security, UKM. She received her PhD in Computer and Information Sciences from the University of Strathclyde, Glasgow. Her main research interests are in the areas of Information Retrieval and Natural Language Processing.

eISSN: 2550-2131
ISSN: 1675-8021