Investigating the Trust Model in the Setting of a Telephone Scam

Sim Hsin Wei Lauren\(^1\), Chan Kar Jan\(^1\), Toh Kai Lin\(^1\) and See Swee Lan\(^2\)

\(^1\) CHIJ St. Nicholas Girls’ School (Secondary), 501 Ang Mo Kio Street 13, S(569405)

\(^2\) Institute for Infocomm Research (I\(^2\)R) A*STAR, 1 Fusionopolis Way, Singapore S(138632)

**ABSTRACT**

Due to advancements in technology, the number of mobile phone users has been increasing drastically. As mobile phones get more accessible, the number of scam cases has also increased greatly. Scams can cause people to be affected emotionally or lose money, which can eventually lead to more serious societal problems. This paper investigates how the friendliness and reputation of a scammer can affect the trust between the scammer and the victim in the setting of a telephone scam, and the words people use when they trust a scammer more. The words were implemented into a technical script, *Ligeia*, which would attempt to decipher the dialogue of potential victims and warn them from falling into telephone scams when they begin to display a high trust level in their word use. An experiment was performed using mixed method research. Data was collected through an online survey with 100 responses, and then analysed using the SPSS and Nvivo 11 softwares. Results showed that both reputation and friendliness are factors of Trust in telephone scams, and words that indicate trust from victims to scammer tend to include words of positive connotation.

**BACKGROUND**

Commercial scams in Singapore increased from 5,687 cases in 2014 to 8,329 cases in 2015, with a 46.5% increase\(^1\). This shows the urgent need to solve this growing problem anyone could fall victim to. Trust is an important factor in telephone scams\(^2\). In our study, Trust is defined as the ‘psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another’\(^3\). This definition would be highly applicable in the case of telephone scams, in which victims unconsciously place themselves in a state of vulnerability by being taken in by the words of the other party, thus being susceptible to the actions of the perpetrator. This study discusses how the friendliness and reputability of someone affect trust and how they manifest in the form of words used in a speech. The study focuses on an investment fraud scam, and covers how much one will trust a stranger he or she does not know based on the stranger’s friendliness (willingness to show concern and be pleasant and personable on his/her own accord) and reputability (the perceived reliability of the stranger (organisation)). From the results, we attempt to propose a solution for this problem, that is, to develop a technical script (*Ligeia*) that could be installed on smartphones to help track the trust level of victims while on the phone and warn them against falling into a scammer’s trick and/or trap. In this way, this would lower the chances of people getting scammed.

**HYPOTHESES**

In order to study how we could develop a technical solution to help lower a person’s chances of being scammed, we have formulated the following hypotheses after performing a literature analysis on the topic of trust.
**Hypothesis 1 (H1): Reputation is a factor of Trust in telephone scams, having a positive influence on trust formed**

Reputation is a possible factor affecting Trust in an E-commerce setting [4]. The paper defines trust as a critical factor in stimulating purchases over the Internet, but can only exist if the consumer believes that the seller has both the ability and the motivation to deliver goods and services of the quality expected by the consumer. This shows that the consumer needs to believe that the seller is reliable, meaning that the seller has a good reputation, to buy a product from that seller. This is very applicable to a telephone scam setting as victims do not know much about the scammers, and are unlikely to see them scammers face-to-face as video calls are used much less often than voice calls, especially with strangers. This will result in higher trust when a familiar name or brand is mentioned in the conversation, as the credibility and trust associated with that organisation will also influence the trust levels of the victim in the conversation.

**Hypothesis 2 (H2): Friendliness of the scammer is a factor of Trust in telephone scams, having a positive influence on trust formed**

Many social factors like benevolence [5], benevolent concern and level of communication [6], and social interactions [7], play a role in building trust between two people. They reduce the perception of the risk of trusting another party, which helps in building trust. By showing concern to the other party and building social bonds, one will be more inclined to feel that the other party will act in their interest. In telephone scams, the victim does not know the real intentions of the scammer. Thus, if the scammer displays more friendliness during the conversation, it will help to convince the victim that they are trying to look out for the victim’s interests and result in the victim being more inclined to trust the scammer.

**Hypothesis 3 (H3): Words that indicate trust from victims to scammer tend to include words of positive connotation (e.g. yes, sure)**

Telephone scams rely heavily on the words that the scammer uses to convince the victim since body language or facial expressions do not come into play. To gain the victim’s trust, scammers would have to give them a positive impression which would be through words and speech features. This is because if there is trust between two strangers, it will be categorised under ‘calculus-based trust’ [8] which involve both parties being careful with their words and the impression they give off to preserve trust. The victim will then want to build mutual trust with the scammer with words associated with positivity in a telephone conversation setting.

This would alleviate the problem of people being affected emotionally and financially due to telephone scams.

**METHOD AND MATERIALS**

We employed a mixed-method research method to carrying out the investigation. To answer the three hypotheses above, we collected both quantitative and qualitative data for analysis through the use of an online survey.

The present study was approved by IRB. The survey was designed to test our hypotheses on friendliness and reputability and its impact on trust. We consider using an online form in our experiment as similar to using a traditional telephone call for in both cases, the respondent does not see the other party’s face and body language, thereby minimising external influence.
However using an online form has an added advantage for it can help us to quickly reach a larger group of participants.

The survey used four different recordings, namely:

*Recording A:* Control recording, not a real scam.
*Recording B:* Recording manipulated by use to include use of friendliness and reputability
*Recording C:* Recording manipulated by use to include use of reputability
*Recording D:* Recording manipulated by use to include use of friendliness

The manuscript we used in the survey recordings was adapted from a real life investment fraud scam situation [9]. *Reputability* is incorporated into the script by adding names of companies or places, and statistics to make the investment sound more legitimate. *Friendliness* is incorporated through concern for the recipient's wellbeing and benefits by being more informal.

The four recordings used in the survey were recorded in a male voice for there could be more male scammers than female scammers [10].

Participants were asked to rank their trust levels for each recording (quantitative) and respond to the recordings they trust the most and the least (qualitative). These participants were aged 13 to 85 years old, from both genders and all racial groups. They were convenient sample and volunteers from the experimenters’ social network.

### RESULTS

#### A. Online Survey

A total of 100 responses were collated and analysed quantitatively using the Statistical Package for the Social Sciences software (SPSS) and qualitatively using the NVIVO software [11].

![Fig. 1 Percentage of people who trusted each recording the most](image1)

![Fig. 2 Percentage of people who trusted each recording the least](image2)

Fig. 1 and Fig. 2 showed that people generally did not trust the recordings that were friendly, which were Recordings B and D, but trusted the ones that were only reputable, which was Recording C. The highest percentage of people trusted Recording A, the control.
The participants were also asked for reasons why they trusted or distrusted a recording. Recording C was the most trusted because the speaker stated that his company was certified by a security company as the best and that he was able to send different relevant documents to inform more about the company he was working for. This shows that access to credible information is important to people as it makes them think that the other party is legitimate and will carry out promises made, hence deciding to place their trust in them.

Recording D was the least trusted because it did not sound credible as the company name was not stated. It also failed to mention any relevant documents or places to obtain more information and the qualifications of the company. The people who participated in this survey thus found this the least reputable and did not trust it.

Friendliness does not have a great impact on the decision to trust a scammer, possibly because it is something very subjective. People can have different definitions of friendliness and interpret and respond to it differently. Something that seems friendly to one person can seem unfriendly to another. Similarly, some may find friendliness appealing and think the speaker is helpful and enthusiastic, while other think that being friendly is suspicious as it sounds too casual, which may mean the speaker is unprofessional and hence unreliable.

In the survey, the participants were also asked to evaluate how friendly and reputable each recording is, as well as how much they trust each recording. Friendliness and reputability were evaluated based on a linear scale from 1 to 5, with 1 being not friendly and not reputable at all, and 5 being extremely friendly and reputable. Trust was evaluated based on a linear scale from 0 to 5, with 0 being not trustable at all and 5 being extremely trustable.

Based on the results, the data was analysed such that for trust, 0-2 was considered as distrust and 3-5 was considered as trust. For reputability and friendliness, 1-2 was considered as not reputable and friendly, whereas 4-5 was considered as reputable and friendly. 3 was regarded as neutral and disregarded in the calculations. The ratio of positive to negative responses for each component was calculated and expressed as percentages in the table below.

<table>
<thead>
<tr>
<th>Recording</th>
<th>No. of people recording is trusted by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Do not trust</td>
</tr>
<tr>
<td>A</td>
<td>47</td>
</tr>
<tr>
<td>B</td>
<td>64</td>
</tr>
<tr>
<td>C</td>
<td>42</td>
</tr>
<tr>
<td>D</td>
<td>71</td>
</tr>
</tbody>
</table>

Table 1 Comparison of recordings A, B, C and D

From Table 1, Recording C was seen as most reputable and was also the most trusted. Recording D was seen as most friendly, but was trusted the least. Comparing the results, the more reputable the recording is perceived to be, the more trusted it is.

Results from SPSS showed that reputability affects trust to a large extent while friendliness only affects trust to a small extent.
To assess the size and direction of the linear relationship between reputability and trust, and friendliness and trust, a bivariate Pearson’s product-moment correlation (r) was calculated. The bivariate correlation between reputability and trust was positive, \( r(98) = .827, p < .001 \). With \( r^2 = 0.684 \), this effect size showed that 68.4% of variance in trust can be accounted for by reputability.

Similarly, the bivariate correlation between friendliness and trust was also positive, \( r(98) = .440, p < .001 \). With \( r^2 = 0.194 \), this effect size showed that only 19.4% of variance in trust can be accounted for by friendliness, which is smaller than reputability.

From SPSS, the assumptions of normality, linearity and homoscedasticity were also not violated. A visual inspection of the normal Q-Q and detrended Q-Q plots for each variable confirmed that both were normally distributed. Similarly, a visual inspection of a scatterplot of trust against reputability and a scatterplot of trust against friendliness confirmed that these two relationships were linear and heteroscedastic.

---

**Table 2 Results of bivariate correlation between reputability and trust**

<table>
<thead>
<tr>
<th></th>
<th>level of trust Pearson Correlation</th>
<th>.827**</th>
<th>( r = .827 ), ( p &lt; .001 )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3 Results of bivariate correlation between friendliness and trust**

<table>
<thead>
<tr>
<th></th>
<th>level of trust Pearson Correlation</th>
<th>.440**</th>
<th>( r = .440 ), ( p &lt; .001 )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

**Correlations**

<table>
<thead>
<tr>
<th></th>
<th>friendliness Pearson Correlation</th>
<th>.440**</th>
<th>( r = .440 ), ( p &lt; .001 )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

**Correlations**

---

![Fig. 3 Relationship between reputability and trust](image1)

![Fig. 4 Relationship between friendliness and trust](image2)
Fig. 3 shows the relationship between reputability and trust. It can be seen that there is a positive and linear correlation between the two, where the more reputable the scammer is, the more the victim would trust the scammer. The trust increases up to a certain point whereby the scammer is perceived as quite reputable, after which, the trust level remains the same even though perceived reputability may increase. This may be because the trust of the victim towards the scammer, a stranger, is limited. Since the victim does not personally know the scammer and his personality, the victim has no way of knowing the true reputability of the scammer. Hence, no matter how highly perceived the scammer’s reputability is the victim will not totally trust the scammer.

Fig. 4 shows the relationship between friendliness and trust. It is observed that there is a positive correlation between friendliness and trust, up to when the perceived friendliness is four, where the trust level then dropped to zero. This showed that trust levels increase with friendliness, however, with higher perceived friendliness levels, the trust levels may decrease instead. This is possibly because how friendly a person is being is subjective and differs from person to person. Therefore, perceived friendliness affects trust positively, until a certain point, where it can cause distrust.

B. Text Analysis
Using the 11th edition of the NVivo software [11], the responses of participants to the recordings they trust the most and the least were analysed and the frequency of the words used were retrieved. The respondents were considered potential ‘victims’. These words from these potential victims were then incorporated into the survey recording script to identify high trust levels in victims with to warn them of the possibility of a scam.

For the recording trusted the most, respondents used ‘think’ or ‘consider’ the most, a total of about 24 times. This was followed by ‘please’, which appeared 14 times. ‘Contact’ and its synonyms, like ‘meet’ and ‘call’ also appeared a total of 14 times.

For the recording trusted the least, respondents used ‘not interested’ the most, a total of 31 times. ‘Sorry’ appeared the second most, with a total of 30 times. ‘No thank you’ or ‘no thanks’ was the third most common, appearing a total of 25 times.

All the words mentioned above were considered as the likely words people could reply or say more when they trust or distrust a scammer as they appeared as high-frequency words.

Words such as ‘investment’, ‘company’ were disregarded as these were considered as neutral words specific to the context. They also appeared roughly the same number of times in the responses to both recordings. ‘Bye’ was also ignored as it is commonly used in phone calls as a farewell.

Positive is defined as looking towards the good side of things, showing approval and interest, while negative is defined as looking towards the bad side of things, showing refusal and disinterest. Neutral words do not imply anything, showing neither interest nor disinterest. ‘Think’, ‘consider’, and ‘contact’ and its synonyms imply that one is willing to learn more about the offer, displaying slight interest, which shows that it is a positive term. ‘Please’ hints at politeness in the conversation, but shows neither interest nor disinterest as it can be used in multiple contexts. However, term such as “no thank you” displayed no interest in the matter and thus counted towards the negative side of words.
Most of the words spoken when trust levels were high do contain a positive connotation, showing interest in the offer, while the words when trust levels were low show no interest.

The words were also analysed within the different age groups to find similarities and differences between words spoken more often in different age groups. This would show if people of different age groups have similar or different ways of speaking.

<table>
<thead>
<tr>
<th>Age group</th>
<th>13-20yrs old</th>
<th>21-35yrs old</th>
<th>36-50yrs old</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most common word used¹</td>
<td>Trust</td>
<td>Distrust</td>
<td>Trust</td>
</tr>
<tr>
<td>1st</td>
<td>Thank</td>
<td>No thanks</td>
<td>Look</td>
</tr>
<tr>
<td>2nd</td>
<td>Investment</td>
<td>Not interested</td>
<td>*</td>
</tr>
<tr>
<td>3rd</td>
<td>Information</td>
<td>Sorry</td>
<td>*</td>
</tr>
</tbody>
</table>

¹Stemmed words were included
*The rest were tied

Table 4 Comparisons of most common words used across different age groups

In general, the 36-50 age group was more concerned about money as investment for trust and in the context of money, for distrust were part of their most commonly used words. The 13-20 and the 21-35 age groups were more direct, having “not interested” as one of their most common words for distrust. The 13-20 age group seemed to be more polite, as “thanks” and “no thanks” were the most common words they used for expressing trust and distrust respectively.

C. Hypotheses
From the results, the perceived reputation of the scammer to the victim has positive impact on trust, so the first hypothesis, \( H_1: \) Reputation is a factor of Trust in telephone scams, having a positive influence on trust formed) was accepted. Friendliness has a small positive impact on trust in the setting of telephone scams, so the second hypothesis, \( H_2: \) Friendliness of the scammer is a factor of Trust in telephone scams, having a positive influence on trust formed) was accepted. The words that indicate trust from victims to scammer do include words of positive connotation, so hypothesis, \( H_3: \) Words that indicate trust from victims to scammer tend to include words of positive connotation) was also accepted.

D. Technical Script (Ligeia)
With the increasing scam cases, our results supported us to developing a solution to help reduce these scams. A technical script named Ligeia is proposed. Developing using C++, Ligeia is based on our research findings and to focus at detecting potential threat in investment fraud scam or similar scams. The model that was built up runs on Windows, but this idea can be applied to the android operating system, which hopefully can be made available at the PlayStore for download to use.

Ligeia would recognise the words the speaker (victim) says and converts it to text (see Fig. 5) We have designed it to recognise the words of the victim only, and not the scammer, because each person gets affected by a scammer's words differently. That is, some people may be persuaded, some people may be less swayed, making it more accurate and effective to detect trust levels from the victim’s words instead. Ligeia will then count the number of times the speaker says the selected words, and beep when the words that indicate trust are one and a
half times the words that indicate distrust, or when the number of trust words is above two (see Fig. 6)

Fig. 5 Ligeia recognising speech input

```
--- Partial result received by OnPartialResponseReceivedHandler() ---
I will consider this and get back to you if I am interested.
--- Partial result received by OnPartialResponseReceivedHandler() ---
I will consider this and get back to you if I am in
--- Partial result received by OnPartialResponseReceivedHandler() ---
I will consider this and get back to you if I didn't
--- Partial result received by OnPartialResponseReceivedHandler() ---
I will consider this and get back to you if I am interested
--- Partial result received by OnPartialResponseReceivedHandler() ---
I will consider this and get back to you if I am interested
```

-- Final n-BEST Results -----
[0] Confidence=High, Text="I will consider this and get back to you if I am interested."
[1] Confidence=High, Text="I will consider this and get back to you if I'm interested."
[2] Confidence=High, Text="I will consider Alpha and get back to you if I am interested."
[3] Confidence=High, Text="I will consider Alpha and get back to you if I'm interested."
[4] Confidence=High, Text="I will consider this up and get back to you if I am interested."

think = 0
consider = 1
contact = 0
call = 0
meet = 0
get back to = 1
learn more = 0
consideration = 0
----- Count A words = 2
not interested = 0
sorry = 0
no thank you = 0
no thanks = 0
----- Count B words = 0
Ratio = oo
=====> Trusted!!

Fig. 6 Ligeia counting number of words indicating trust and distrust

Before the requirement is met, there is insufficient information to tell whether the victim trusts the scammer, as we are only relying on words. This also reduces the occurrences of unnecessary beeping that may disrupt people’s conversations. After the requirement is met, it will be quite clear that the victim is starting to trust the scammer, and needs a warning to prevent him/her from fully trusting the scammer.

**DISCUSSION**

**A. Online Survey**

From our results, we found that reputability did affect trust positively, where the more reputable the recording was thought to be, the more it was trusted. Many scammers claimed that they are from a well-known and trusted company, to get victims to fall for their scams. For example, there was an incident in 2016, where a scam survey used the name of a well-
known supermarket in Singapore [12]. Our findings explained why scammers identify themselves from a large and reputable company rather than a fictitious organisation.

However, the friendliness of the recording only affected how much it was trusted to a small extent, possibly due to the subjectiveness of friendliness. To some people, a person being friendly can make them seem more passionate about the subject matter, convincing the person to continue listening. However, friendliness may seem suspicious to others, who think they are not taking the subject matter seriously, hence distrusting them. This may be affected by one’s personality or age group. For example, if a person tends to overthink or ask many questions, he or she is less likely to trust a scammer. If the victim is less curious or tends to take things at face value, he or she may trust a scammer more. The age group can also affect one’s tendency to trust. For example, elderly in Singapore may be more likely to trust a friendly recording than others as they may be more used to talking to strangers they meet in public. Words that the scammer uses may also unconsciously cause the victim to trust him, as each generation has a rather distinctive way of speaking. Trust in a salesperson is dependent on how relatable the salesperson is to the customer [9]. Thus, by using slang words while talking to the youths may cause them to trust more since they have similar speaking styles.

All in all, understanding the key factors that affect people to trust scammers is important. For instance, since we know that the scammer’s reputation is a key factor of trust in a scammer, to prevent scams, we should attempt to prevent people from falling prey. Through the use of technology, hopefully one possible solution that we proposed in this paper could help, and with further improvement, could be effective.

B. Text Analysis
We also found that words indicating trust were in fact mostly positive and expressed interest, while words mostly expressing disinterest indicated distrust in the investment offer. This can also be seen when people receive calls promoting or advertising products, and people responded with “no thank you”. This showed that people do not wish to buy or invest in the product, like when one does not trust a scammer. However, if a person would like to buy the product, he or she would want to know more about it, and thus show interest. Having deciphered the commonly said words when there are of high trust and interest levels, they can be used in a programme to convince one to reconsider an offer when high trust levels are detected.

C. Future Research Directions
Further improvements can be made to perform a more in-depth study.

Firstly, we could reach out to more middle-aged and elderly people, since respondents in the present study were mainly from the younger age ranges. Since the elderly get targeted more by scammers [13], Ligeia would be more helpful to them, and thus having more information about what words the elderly use when they distrust or trust a phone call and also what factors make them trust the scammer would make Ligeia more effective for them.

Secondly, the survey could have been done in more of a conversational style, similar to actual phone calls, so as to make the experience more authentic and the results more accurate. However, this would have had to be done over the phone for the respondent to only focus on the words, and that would not have been very practical, as it would be too time-consuming or result in inaccurate responses should people want to get off the phone quickly.
In future, the trust model in the setting of other types of scams can also be explored, such as free vacation scams, where one is told to pay a tax price to redeem a free vacation. This is similar to investment fraud scams as they are common and do not require face-to-face interaction. Other factors can also be tested for its effect on trust in telephone scams, like the scammer’s tone, the victim’s socio-economic class, etc. The technical script, Ligeia, can further be improved to identify the trust level of victims in other types of scams, and in other languages too.

CONCLUSION
In summary, we conclude that both the reputation and friendliness of a scammer are critical factors of Trust in telephone scams. Words that indicated trust from victims to scammer tend to include positive words. A technical script, Ligeia, identifying words indicating trust and distrust was proposed and under development for further testing. This would hopefully help to warn people before they are scammed, thus contributing to lessening the societal problems that scams can cause.

ACKNOWLEDGEMENTS
We would like to thank the Ministry of Education (MOE), Singapore, A*STAR (I2R) and CHIJ St. Nicholas Girls’ School (Secondary) for giving us this opportunity to research on this project through the Science Mentorship Programme (SMP).
REFERENCES
APPENDIX

(I) Survey: This is accessible at
https://docs.google.com/forms/d/15xmd78zyA9OYLrXlrDPrXo9USIKUD4jkP1ZkmCUoJ-4/edit?usp=sharing

(II) Transcript: This is accessible at:
https://docs.google.com/document/d/1F95pHnJUzH2YD15aqSQip4tKdi3KV3eAHthejVv_v7A/edit?usp=sharing