Annual ADFSL Conference on Digital Forensics, Security and Law

2007
Proceedings

Investigating Information Structure of Phishing Emails Based on Persuasive Communication Perspective

Ki Jung Lee
The iSchool at Drexel, College of Information Science and Technology, Drexel University, Philadelphia, PA USA

Il-Yeol Song
The iSchool at Drexel, College of Information Science and Technology, Drexel University, Philadelphia, PA USA

Scholarly Commons Citation

Lee, Ki Jung and Song, Il-Yeol, "Investigating Information Structure of Phishing Emails Based on Persuasive Communication Perspective" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 2.
https://commons.erau.edu/adfsl/2007/session-12/2

Investigating Information Structure of Phishing Emails Based on Persuasive Communication Perspective

Ki Jung Lee
The iSchool at Drexel
College of Information Science and Technology
Drexel University
Philadelphia, PA USA

Il-Yeol Song
The iSchool at Drexel
College of Information Science and Technology
Drexel University
Philadelphia, PA USA

ABSTRACT

Current approaches of phishing filters depend on classifying messages based on textually discernable features such as IP-based URLs or domain names as those features that can be easily extracted from a given phishing message. However, in the same sense, those easily perceptible features can be easily manipulated by sophisticated phishers. Therefore, it is important that universal patterns of phishing messages should be identified for feature extraction to serve as a basis for text classification. In this paper, we demonstrate that user perception regarding phishing message can be identified in central and peripheral routes of information processing. We also present a method of formulating quantitative model that can represent persuasive information structure in phishing messages. This paper makes contribution to phishing classification research by presenting the idea of universal information structure in terms of persuasive communication theories.

1. INTRODUCTION

In our modern day lives, the internet is a unified window to various sources of information for entertainment, study, healthcare, and many other human created forms of knowledge products. Emails, as a major method of internet communication, serve as a personalized channel of communication for the users to experience such knowledge products in various serviceable forms. Unfortunately, however, emails are being misused by criminals such that they appeal to user's cognition by engineering urgency, authority, or fear in the email message, induce the user's mindless response, and steal proprietary information such as credit card numbers or social security numbers. Such online crime is referred to as phishing.

Phishing is online identity theft in which confidential information is obtained from victims (Emigh, 2005; Kirda & Kruegel, 2006). The crime, moreover, is spreading fast with the increased share of electronic market place in the retail market. According to the research conducted by Gartner Research Group (2005), an estimated 73 million U.S. adults who use the Internet identified that they received or thought they received an average of more than 50 phishing e-mails from June 2004 to May 2005. That number represents a growth rate of 28 percent compared with the previous 12-month period, during which 57 million U.S. adults reported they definitely received or thought they received a phishing e-mail. Phishing scam is a serious problem for many industries since it has a great impact on the internet business which is based on the ring of trust between vendors and consumers. It, coupled with increasing disclosure of unauthorized access to sensitive consumer data, causes a bad influence on consumer confidence in making transactions electronically. Companies are worried that they will lose the ability to leverage low-cost electronic communication channels with their customers.

Phishing attacks are logistically distinct from spam in that 1) phishing attacks are more sophisticated, 2) phishing messages are more likely targeted to specific audience, 3) phishing attacks are more likely to be short-lived, and

4) phishing related web sites are dynamically changing (MessagingAnti-AbuseWorkingGroup & Anti-phishingWorkingGroup, 2006). Technically, therefore, spam filters are not the best solution for phishing filtering. In other words, phishing messages are not easily detected by spam filters since the messages tend to emulate the information structure of legitimate emails. Consequently, some studies identified phishing specific features and systems were designed accordingly. Some of the phishing specific features are IP-based URLs, age of domain names, non-matching URLs, number of links, number of domains, number of dots, and use of javascript (Drake, Oliver, & Koontz, 2005; Fett, Sadeh, & Tomasic, 2006). However, it can be argued that easily discernable features in text, in the same sense, can be easily manipulated by sophisticated attackers. Updating such phishing features for up-to-date design of phishing filter can be cumbersome since criminals can use infinite number of ways to manipulate email messages. Therefore, identifying a fundamental and universal information structure of phishing messages and designing a set of features for such information structure are essential. The motivation of this study is urged by answering the following two fundamental questions in regards to representing the information structure of phishing messages:

1. *Why do people keep deceived by phishing scams?*
2. *What is the universal pattern of phishing message that can be applied to different phishing messages?*

This study finds explanation of phishing victim's mindless response from dual process cognition models. Instead of arguing that heuristic aspect of cognitive process is responsible for user's mindless response, in this paper, we demonstrate that some combinations of dual cognitive processes are related to user's trust decision. This paper analyzes phishing email messages in the user perception level and presents a quantitative model. First, we classify information structure in phishing email messages based on the variables measuring components of persuasive transactions. Then, based on the identified persuasive transaction variables representing dual cognition , in addition to phishing related variables, we compute a quantitative model that can represent the combination of dual cognitive processes while providing the binary prediction whether the message is phishing or not. From the outset, we argue that the key to the ultimate solution of phishing scam can be found from people, i.e., the users. Since phishing attacks mainly depend on user's mindless response to manipulated email messages (i.e., socially engineered messages), the victims play a fundamental role in the crime (Merwe, Loock, & Dabrowski, 2005). Therefore, it is important to know how the social engineering is deployed and used in phishing emails to trick people and how email users perceive manipulated messages and make trust decision.

The objective of this paper is to present a research framework for phishing filter feature extraction. Although different approaches have been investigated to analyze phishing attacks (Adida, Hohenberger, & Rivest, ; Inomata, Rahman, Okamoto, & Okamoto, ; Jakobsson, 2005; Parno, Kuo, & Perrig, 2005), there has not been an attempt to analyze it in user's perception level. This paper provides a framework of a research method in phishing feature extraction based on information structure derived from robust communication theories.

This paper describes a pilot analysis with a small sample size. When a sample size is substantially larger, we expect the same method would provide more refined results in addition to a richer set of descriptive analysis results. The remaining sections are organized as follows: Section 2 reviews theoretical background of this study. In Section 3, the research procedure and variable selection are discussed. In Section 4, we present the statistical procedure for verifying dual process cognition model and computing binary prediction model. In Section 5, limitations of the current study and further study directions are discussed. Section 6 concludes our paper.

2. THEORETICAL BACKGROUND

In this section, we provide a theoretical background behind our argument that message structures in phishing emails can be examined in terms of persuasive communication theory. Although phishing can be conceptually defined as manipulation, rather than persuasion, they are not too different when it comes to message manipulation tactics and message receiver perception processes. By using the variables measuring persuasive transactions, we can develop a quantitative model that represents the structure of persuasive information in email messages. In a practical sense, phishing emails and legitimate emails will have different combination and/or contribution of the persuasion variables and can be distinguished by the equation containing the set of combination and contribution.

The framework we utilize in this paper is based on persuasive communication perspective in two folds; components of persuasive transaction guiding compliance gaining message production and a user cognitive model that identifies how people would process information in email messages. Components of persuasive transactions concern message sender's message manipulation strategies whereas the user cognitive model concern message receiver's information processing model. In summary, message flows of phishing communication in our argument can be simplified as follows:

Sender message manipulation → Receiver information processing → Receiver trust decision.

2.1. Sender's message manipulation

The art of persuasion has been investigated for several decades since Aristotle defined various ways of persuasive appeals such as logos (i.e., rational appeal), pathos (i.e., emotional appeal), and ethos (i.e., appeal through knowledgeable character). Until today, source characteristics and message characteristics are major components of persuasive communication. However, since we discuss communication by means of computers, persuasive transaction components in this paper are discussed in two broad aspects: Traditional persuasion approaches and persuasive technology perspective which are more recent research topics in relation to persuasive interface design.

2.1.1. Source variables and message variables

Traditionally, message contents are studied as a major factor that influences communication outcome. Hovland et al. (1953), rather than designing a formal theory about message learning, started with "assumptions" of how people learn verbal and nonverbal skills. Their assumptions indicate that a persuasive communication requires a person's attention and comprehension concerning the information in the message. After a person attends to the message and understands it, s/he establishes a connection between the presented issue and those cognitive responses by mentally repeating the message arguments. This repeating may result in storage of information in memory in ways that signify the arguments and conclusion. Although attention, comprehension, and retention are necessary preconditions for attitude change, Hovland et al. define incentive (i.e., reward) as a sufficient precondition. They, in other words, imply that attitude change can occur when major communication stimuli is not directly related to message content.

Source variables and message variables are mainly discussed in this perspective. Source variables are related to the characteristics of message sources in relation to persuasion effectiveness. Source credibility in terms of perceived expertise and trustworthiness is the major concern in the discussion of source variables (Hovland et al., 1953; McCroskey, 1966).

Other kind of traditional variables, discussed in this paper, in relation to sender's message manipulation are message variables. The message variables concern features of messages that are influential in the process of persuasive communication. For example, messages can be rationally appealing to message receivers so that they evaluate evidentiary information. In other cases, messages can be emotionally appealing so that message receivers are influenced by fear or guilt in relation to the message content (O'keefe, 1990; Petty & Cacioppo, 1981; Stiff & Mongeau, 2003).

2.1.2. Computer related variables

More recently, technology factors are also considered as important factors influencing communication outcome. In general, computer interfaces are designed for various purposes such as productivity, entertainment, and communication. Thus, usability is one of the core factors of interface design principles. It focuses on functionality of the interface so that users can complete information transaction without much difficulty if they desire. However, usability is not necessarily a sufficient condition for users to actually make transactions. To be successful in fulfilling the goal of making users actually involved in the transaction, the interface design should reflect persuasive factors which stimulate user's motivation. Current research on persuasive interface design investigates human components in the computer interface which give the users illusory perception as if they were interacting with human being (Fogg, 2003; Reeves & Nass, 1996).

According to the functional triad (Fogg, 2003), computers can play various roles in conveying persuasive influence to the users. First, computer as a tool aids the users in making target behavior easier. For example, one click shopping in some online retail store can appeal to buyers by reducing various steps of activities to a few simple steps. In addition, computer as media can appeal to users by offering vicarious experience. Users can be motivated by experiencing simulated environment by computers. Lastly, computers can influence users by interaction with them as if humans do, namely, social actors.

2.2. Receiver's information processing

The user cognition model in our interest is a dual process of cognition. Dual process models of cognition claim that a person's mode of thinking determines influence on processing of information. The models share assumptions about general ideas: 1) there are two relatively distinct modes of cognitive processing that a person takes, 2) situational and personal variables affect choice of mode, 3) effects are different depending upon the mode of process, and 4) influence achieved through receiver's cognitive effort is more persistent over time, more resistant to change, and more predictive of behavior than the heuristic processing mode ("Dual process persuasion," n.d.).

For the analysis in this paper, we choose Elaboration Likelihood Model (ELM) since it is widely applied to various applications. The ELM is based on the idea that attitudes guide decision-making and its following behavior. The model, therefore, concerns the process to reach the attitude change and how source, message, receiver, and channel factors affect the mechanism of message receiver's cognitive effort in information processing. Petty and Cacioppo (Petty & Cacioppo, 1981) identify that there are two distinctive routes to the information processing which represent the receiver's engagement with various degree of cognitive effort, i.e., central route and peripheral route. The central route concerns the information that a person has regarding an object or an issue. Some of the main factors that the central route focuses are: 1) how the arguments are learned, 2) what kind of information people create, and 3) how people combine new information with prior knowledge. The information processing in this route appears to be rational. Therefore, the message recipient attends to the message arguments and attempts to scrutinize in order to evaluate them. In contrast, the peripheral route reflects a very different notion of information processing. Attitude change is determined by: 1) rewards or punishments that are associated with the message, 2) simple inferential cues, and 3) judgmental errors that occur in perceiving message. In the peripheral route, message perceivers make judgments based on simple cues that source or message provide.

The primary difference between the two routes is whether the perceiver engages in active thinking regarding the issue relevant information or not. In other words, the central route is taken if a perceiver engages in cognitive effort to process the issue relevant information, whereas the peripheral route is taken when simple cues are applied with significantly less cognitive effort than the central route. Therefore, the persuasive effects are distinct depending on the two routes: influence achieved through receiver's cognitive effort is more persistent over time, more resistant to change, and more predictive of behavior than peripheral processing route. In general, however, the peripheral route deems to produce persuasive outcome more easily because people tend to make quick decisions based on peripheral cues.

2.3. Research questions

Based on the previous discussion on persuasive transactions and dual process of cognition, we state the following two research questions:

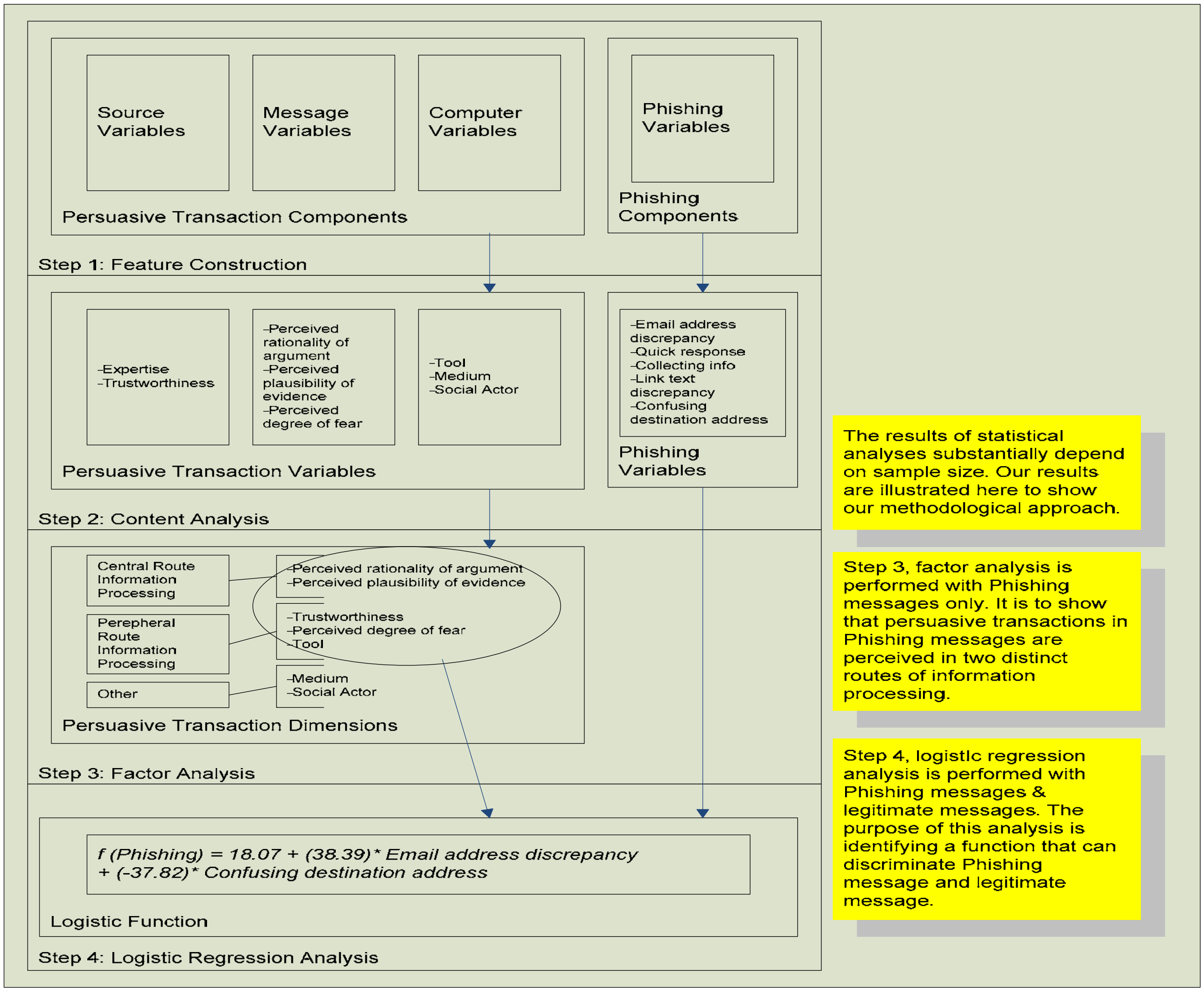
(1) Would the persuasive information structure in phishing message be perceived in two distinct routes by the email recipients?
(2) Would the persuasive information structure in phishing message serve as good features for classifying phishing message from legitimate message?

Designing a research study and testing collected data for the aforementioned research questions involves two statistical analyses, i.e., factor analysis and logistic regression analysis. Factor analysis identifies underlying dimensions among a set of variables. Therefore, in order to test the dual process information processing, stated in the research question (1), we conduct a factor analysis. In addition, logistic regression analysis is used for categorization and prediction. For designing of potential formula for classifying email messages, required for answering research question (2), binomial logistic regression is used.

3. METHOD

In this section, we present the procedures and measures that are used in our analyses. Sampling procedure, sample selection, content analysis procedure, and measurements are discussed. Our main method consists of four steps; 1) feature construction, 2) content analysis, 3) factor analysis, and 4) logistic regression analysis. Figure 1 illustrates procedures of our methodological approach.

Figure 1 Methodological approach of our study


Source Variables
Message Variables
Computer Variables
Persuasive Transaction Components
Phishing Variables
Phishing Components
Step 1: Feature Construction
-Expertise
-Trustworthiness
-Perceived rationality of argument
-Perceived plausibility of evidence
-Perceived degree of fear
-Tool
-Medium
-Social Actor
Persuasive Transaction Variables
-Email address discrepancy
-Quick response
-Collecting info
-Link text discrepancy
-Confusing destination address
Phishing Variables
Step 2: Content Analysis
Central Route Information Processing
Perepheral Route Information Processing
Other
-Perceived rationality of argument
-Perceived plausibility of evidence
-Trustworthiness
-Perceived degree of fear
-Tool
-Medium
-Social Actor
Persuasive Transaction Dimensions
Step 3: Factor Analysis
f (Phishing) = 18.07 + (38.39)* Email address discrepancy + (-37.82)* Confusing destination address
Logistic Function
Step 4: Logistic Regression Analysis

The results of statistical analyses substantially depend on sample size. Our results are illustrated here to show our methodological approach.

Step 3, factor analysis is performed with Phishing messages only. It is to show that persuasive transactions in Phishing messages are perceived in two distinct routes of information processing.

Step 4, logistic regression analysis is performed with Phishing messages & legitimate messages. The purpose of this analysis is identifying a function that can discriminate Phishing message and legitimate message.

3.1. Sample Collection

Phishing emails were collected by email feeds from antiphishing.org. Email feeds are received through info620@gmail.com which was set up particularly for this project. The feeding began from Aug 16, 2006 adding thousands of feedings per day. Since the email feedings of antiphishing.org are provided by members who are not necessarily well aware of the definition of phishing, some feedings were not phishing emails. Among the provided feedings, reasonably identifiable as phishing emails are selected in our sample. The sample for equation generation includes both phishing emails and legitimate emails. Legitimate emails are collected from personal email accounts.

3.2. Variables and Procedures

Variables used for our analyses were selected from a series of studies identified below. Source variables, message variables, and computer variables are measured in the five point Likert scale anchoring from 1, not likely, to 5, very likely. Phishing variables are coded in a binary form to simply represent the existence of the particular feature. Brief description of each variable is illustrated in Table 1, and the selection of variables followed descriptions below.

- Source variables and message variables are selected from reviewing persuasion literature (Hovland et al., 1953; McCroskey, 1966; O'keefe, 1990; Stiff & Mongeau, 2003).
- Computer variables are derived from Fogg's functional triad (Fogg, 2003).
- Phishing variables are selected from reviewing phishing related literature (Drake et al., 2005; Fett et al., 2006)

Table 1 Description of variables used in analyses

Kind of Analysis		Used Variable Components	Used Variable Item Category	Used Variable Item Measurements
Logistic Regression	Factor Analysis	Source variables (Continuous)	Credibility	Expertise Trustworthiness
		Message variables (Continuous)	Rational appeals	Perceived rationality of argument Perceived plausibility of evidence
			Emotional appeals	Perceived degree of fear
		Computer variables (Continuous)	Tool	Easiness of interaction
			Medium	Vicarious experience
			Social actor	Social experience
		Phishing variables (Binary)	Email address discrepancy	Reply address differs from the claimed sender
			Quick response	Requiring a quick response
			Collecting info	Collecting information in the e-mail or links to web sites that gather information
			Link text discrepancy	Link text in e-mail differs from link destination or hides link
			Confusing destination address	Uses @ symbol to confuse

For different analysis, different set of data was used. For factor analysis, five different phishing emails were shown to coders. The messages were evaluated by ten coders based on variables associated with persuasive transactions. Comrey and Lee (1992) recommend more than 300 cases as decent sample size for Factor Analysis. It is generally understood that observation under 10 can cause computational difficulties. Coders spent approximately two minutes to read one email message. After reading the five emails, coders were asked to evaluate their impressions about the phishing emails. For logistic regression analysis, 16 phishing emails and 8 legitimate emails were used. The emails used from logistic regression analysis were selected from different pool so that they do not overlap with the previous five emails shown to the coders. The coding materials and coding results were delivered electronically. The coders received instruction, questionnaire, and the emails for analysis through their emails and the coding results were also submitted via emails.

4. ANALYSES AND RESULTS

In this section, we describe statistical procedures and methods used for our analyses. Analyses of collected data consist of two major procedures. First, factor analysis is used for variable classification. Variables are classified for the validation of a dual process of cognition. From the pool of persuasive communication variables, we identify underlying dimension (see Table 2). Once the variables are classified, cases are classified by conducting logistic regression analysis based on the identified variables as a result of confirmatory factor analysis in addition to known phishing factors described in the previous section. The purpose of case classification is to design a quantitative model that can make predictions on email messages whether they are phishing or not. Known phishing factors are also refined based on close examination. For example, company logo factor is filtered out since both legitimate emails and phishing emails use company logos in their messages. In other words, a company logo is not a good predictor of discriminating phishing emails from legitimate ones. Logistic regression analysis offers the proportion of variance in the dependent variable accounted for by the predictor variables as well as the relative rank of importance of each predictor variable.

Table 2 Factor Loadings - Rotated Component Matrix

Rotated Component Matrix(a)			
	Component		
	1	2	3
Perceived Expertise	0.55	0.50	-0.52
Perceived rationality of argument	0.42	0.07	0.69
Perceived plausibility of evidence	0.02	0.09	0.97
Perceived Trustworthiness	0.42	0.81	0.14
Emotional Appeal (e.g., fear)	0.44	-0.63	-0.30
Easiness of interaction	0.16	-0.72	0.07
Vicarious experience	-0.77	0.06	-0.14
Social experience	-0.84	0.04	-0.11
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.			
a	Rotation converged in 5 iterations.		

4.1. Factor Analysis

Phishing email persuasive message data were examined by a factor analysis using Principal Components extraction and Varimax rotation method. Three factors were extracted and rotated. Each factor was apparently interpretable in terms of distinct characteristic; Factor 2 represents "peripheral route of information processing" whereas Factor 3 concerns the "central route of information processing". Factor 1 was identified with variables that have relatively high factor loading values. It seems that computer variables are separately identified in the user's information processing scheme of persuasive message[1]. The three-factor solution accounted for 73.11 percent of total variance.

The sum of squared loading after rotation for Factor 2 and Factor 3 are 1.84 and 1.83, respectively. These two factors contribute 45.87% of the total variance. Factor 2 was composed of variables indicating user's peripheral route of information processing such as "perceived trustworthiness", "emotional appeal", and "easiness of interaction", each reflecting factor loadings of .81, -.63, and -.72, respectively. Factor 3 consisted of variables reflecting user's central route of information processing such as "Perceived rationality of argument" and "Perceived plausibility of evidence", each having factor loadings of .69, and .97, respectively. The sum of squared loading after rotation for the factor 1 is 2.17, consisting of variables reflecting illusory experience with computer interface. The variables were "Vicarious experience" and "Social experience" with factor loadings of -.77 and -.84, respectively. Factor 1 accounted for 27.23 percent of total variance. "Perceived expertise" loaded similarly to all factors.

The above results show that variables are identified under distinct dimensions. First, "perceived rationality of argument" and "perceived plausibility of evidence" are grouped under a same dimension. We interpret that this dimension represents *central route information processing* since the variables are related to message manipulation that result in more cognitive effort of message receivers when processing information. Second, "perceived trustworthiness," "emotional appeal," and "easiness of interaction" are grouped under a same dimension, representing *peripheral route of information processing*. We argue that they are related to message manipulation resulting in less cognitive involvement when processing main argument of the presented message. "Vicarious experience" and "social experience" are also grouped together. We were not able to provide a proper interpretation of this particular dimension in terms of dual process cognition model. However, we expect that variable grouping can be more refined when the sample size is larger.

4.2. Logistic Regression Analysis

A logistic regression analysis was conducted to examine multivariate predictors of phishing discrimination. Logistic regression can be used to predict a dependent variable on the basis of continuous and/or categorical predictor variables and to determine the percent of variance in the dependent variable explained by the predictors. Logistic regression is a linear classifier, similar to Gaussian Naïve Bayes, that shows function approximation learning algorithms as statistical estimators or functions (Mitchell, 2006; Roos, Wettig, Grunwald, Myllymaki, & Tirri, 2005). With this analysis, a regression equation is created that can predict whether the email is phishing or not.

Since phishing variables are theory-driven and we used different dimensions of variables together in the analysis, we used a forward stepwise method instead of *Enter method* in SPSS management. The predictor variables entered for the analysis are perceived trustworthiness, perceived rationality of argument, perceived plausibility of evidence, emotional appeal, easiness of interaction, vicarious experience, social experience, email address discrepancy, quick response requirement, collecting personal information or not, link text discrepancy, and destination address confusion.

[1] We expect that the pattern would be different with a larger sample size. Current data shows a distinction between traditional persuasive transaction and computer persuasive transaction.

The result identified that the logistic model (100%) had more effective prediction rate than the null model (69.6%). The logistic model was significantly associated with the binary prediction of phishing (χ^2 (2) = 28.26, p<.0001). The suggested equation for the logistic model is stated as below;

$$f\,(\textit{phishing}) = 18.07 + (38.39)^{*}\ \textit{Email address discrepancy} \\ + (-37.82)^{*}\ \textit{Confusing destination address}$$

Furthermore, the insignificant Hosmer–Lemeshow test (□^{2} (1) = 0, p>.05) shows that the null hypothesis of a good model fit to data was acceptable. In other words, the model was a good fit to the data. Therefore, when the data of "Email address discrepancy" and "Confusing destination address" are given we can predict whether the email is phishing or not with 100% accuracy. However, this analysis resulted from only 23 cases of dataset. Since optimal number of observation should be much larger than 23, this analysis only shows methodological approach rather than presenting substantial finding.

5. DISCUSSION

In the sections above, statistical analyses of phishing email structure were presented. Factor analysis classified variables to verify dual process of cognition. Logistic regression analysis presented a potential classifier model that could offer binary prediction. In this section, first, major limitations of this paper are discussed. Although we already identified that this study is for suggesting a research framework, the sample size is an inevitable problem in statistical analysis. Potential limitations of theory adoption and measurement limitation are also discussed.

Without an optimal sample size, this study only shows the research framework instead of significant research results. Unfortunately our preliminary analysis does not result in an equation that contains persuasive transactional components in the predictor variables. Although the result showed that the logistic model would classify phishing with 100 percent accuracy, the equation consists of only phishing features. We expected that the equation would reflect components of persuasion variables when the sample size is large enough since the main point of our argument is that persuasive information structure should work as universal features across different kinds of phishing messages.

In this paper, we only adopted parts of core components of persuasive transactions. In real life situations, more various principles of persuasion can be applied to communications. For example, receiver involvement is a critical component in persuasive communication. If a message receiver is personally involved in the issue presented in the message, it is more likely that the message receiver engage in critical evaluation of the presented message. However, the receiver factor was ignored in our research design since we only looked at sender and message perspectives in that the phishing message was analyzed in terms of sender's message manipulation strategy. However, adoption of persuasive theories may be more refined to consider different perspectives of persuasion.

Measurements used for feature values for this paper was subjective measures which represent user perception. It is a challenging task to represent human perception for the tasks of text classification. System implementation can be difficult and/or uneconomical since there should be an additional system which should function as a reference to signify the feature set representing persuasive component.

6. CONCLUSION

Investigating information structure of phishing email can provide system designers with a novel idea of phishing detecting mechanism. In this paper, we demonstrated that user perception regarding phishing message can be identified in two distinct ways of information processing, i.e., central route and peripheral route. We also identified a quantitative model that represents persuasive information structure in email messages. We claim that the model can be used for classifying phishing emails from legitimate emails. In particular, we proposed a method to design a set of features for the classification based on a dual process model of cognition.

The results of this study indicate that persuasive components in phishing messages can be identified as a set of features for phishing detection mechanism. The results are significant in that the identified set of features using our method can potentially be used for the design of phishing filter which does not required frequent feature update. The features extracted from our method would serve as a universal pattern of phishing email messages.

7. REFERENCES

Adida, B., Hohenberger, S., & Rivest, R. L. Fighting phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails.

Comrey, A. L., & Lee, H. B. (1992). *A First Course in Factor Analysis* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Drake, C. E., Oliver, J. J., & Koontz, E. J. (2005). *Anatomy of a phishing Email*: MailFrontier.

Dual process persuasion. (n.d.). Retrieved October 25, 2005, from http://www.as.wvu.edu/~sbb/comm221/chapters/dual.htm

Emigh, A. (2005). *Online Identity Theft: phishing Technology, Chokepoints and Counter measures*.

Fett, I., Sadeh, N., & Tomasic, A. (2006). *Learning to Detect phishing Emails*.

Fogg, B. J. (2003). *Persuasive technology : using computers to change what we think and do*. Amsterdam ; Boston: Morgan Kaufmann Publishers.

Gartner. (2005). *Increased phishing and Online Attacks Cause Dip in Consumer Confidence*: Gartnet Research Group.

Hovland, C. I., Janis, I. L., & Kelly, J. J. (1953). *Communication and persuasion*. New Haven: Yale University Press.

Inomata, A., Rahman, S. M. M., Okamoto, T., & Okamoto, E. A novel mail filtering method against phishing.

Jakobsson, M. (2005). *Modeling and Preventing phishing Attacks*.Unpublished manuscript.

Kirda, E., & Kruegel, C. (2006). Protecting Users against phishing Attacks. *The Computer Journal*.

McCroskey, J. C. (1966). Scales for the measurement of ethos. *Speech Monographs, 33*, 65-72.

Merwe, A. v. d., Loock, M., & Dabrowski, M. (2005). *Characteristics and Responsibilities involved in a phishing Attack.* Paper presented at the 4th international symposium on Information and communication technologies Cape Town, South Africa.

MessagingAnti-AbuseWorkingGroup, & Anti-phishingWorkingGroup. (2006). *Anti-phishing Best Practices for ISPs and Mailbox Providers*.

Mitchell, T. (2006). Generative and discriminative classifiers: Naive Bayes and Logistic Regression.

O'keefe, D. J. (1990). *Persuasion: Theory and research*. Newbury Park: Sage Publications.

Parno, B., Kuo, C., & Perrig, A. (2005). *Phoolproof phishing Prevention*: CyLab Carnegie Mellon University.

Petty, R. E., & Cacioppo, J. T. (1981). *Attitudes and persuasion: Classic and contemporary approaches*. Dubuque, Iowa: Wm. C. Brown Company Publishers.

Reeves, B., & Nass, C. (1996). *The media equation: How people treat computers, televison, and new media like real people and places*. Stanford, CA: CSLI Publications.

Roos, T., Wettig, H., Grunwald, P., Myllymaki, P., & Tirri, H. (2005). On discriminative Bayesian Network Classifiers and Logistic Regression. *Machine Learning, 59*, 267-296.

Stiff, J. B., & Mongeau, P. A. (2003). *Persuasive communication*. New York: The Guilford Press.