The iSchool at Drexel
Energizing the Infosphere
College of Information Science and Technology

Exploring a method of extracting universal features of phishing emails based on persuasive communication perspective

Ki Jung Lee and Il-Yeol Song

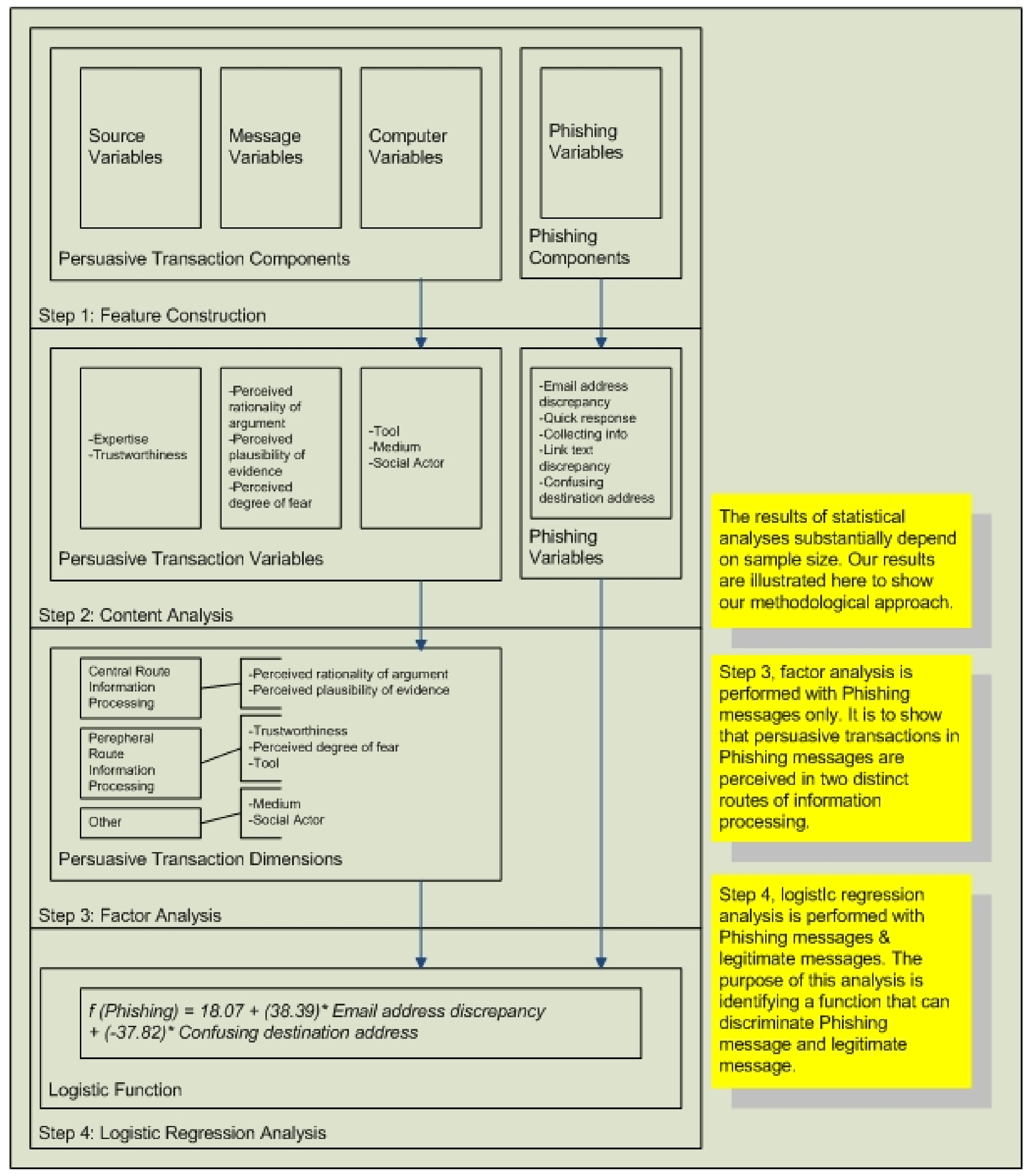
The iSchool at Drexel, College of Information Science and Technology, Drexel University, Philadelphia, PA 19104

ABSTRACT

Current approaches of phishing filters depend on classifying emails based on obviously discernable features such as IP-based URLs or domain names. However, as those features can be easily extracted from a given phishing email, in the same sense, they can be easily manipulated by sophisticated phishers. Therefore, it is important that universal patterns of phishing messages should be identified to serve as a basis for novel phishing classification algorithm.

In this paper, we argue that **phishing is a kind of persuasion** and explore feature extraction method based on persuasive communication perspective. Phishing message components, including **message factors, source factors, and computer related factors**, are investigated as **message sender's strategic message manipulation**. On the other hand, message receiver's cognitive components for information processing are discussed in terms of **dual process of cognition**, i.e., **Elaboration Likelihood Model**.

OVERVIEW


Persuasive Transaction Components: Source Variables, Message Variables, Computer Variables. Phishing Components: Phishing Variables.

Step 1: Feature Construction

Persuasive Transaction Variables: -Expertise -Trustworthiness; -Perceived rationality of argument -Perceived plausibility of evidence -Perceived degree of fear; -Tool -Medium -Social Actor. Phishing Variables: -Email address discrepancy -Quick response -Collecting info -Link text discrepancy -Confusing destination address

Step 2: Content Analysis

Persuasive Transaction Dimensions: Central Route Information Processing: -Perceived rationality of argument -Perceived plausibility of evidence. Perepheral Route Information Processing: -Trustworthiness -Perceived degree of fear -Tool. Other: -Medium -Social Actor

Step 3: Factor Analysis

Logistic Function: f (Phishing) = 18.07 + (38.39)* Email address discrepancy + (-37.82)* Confusing destination address

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.

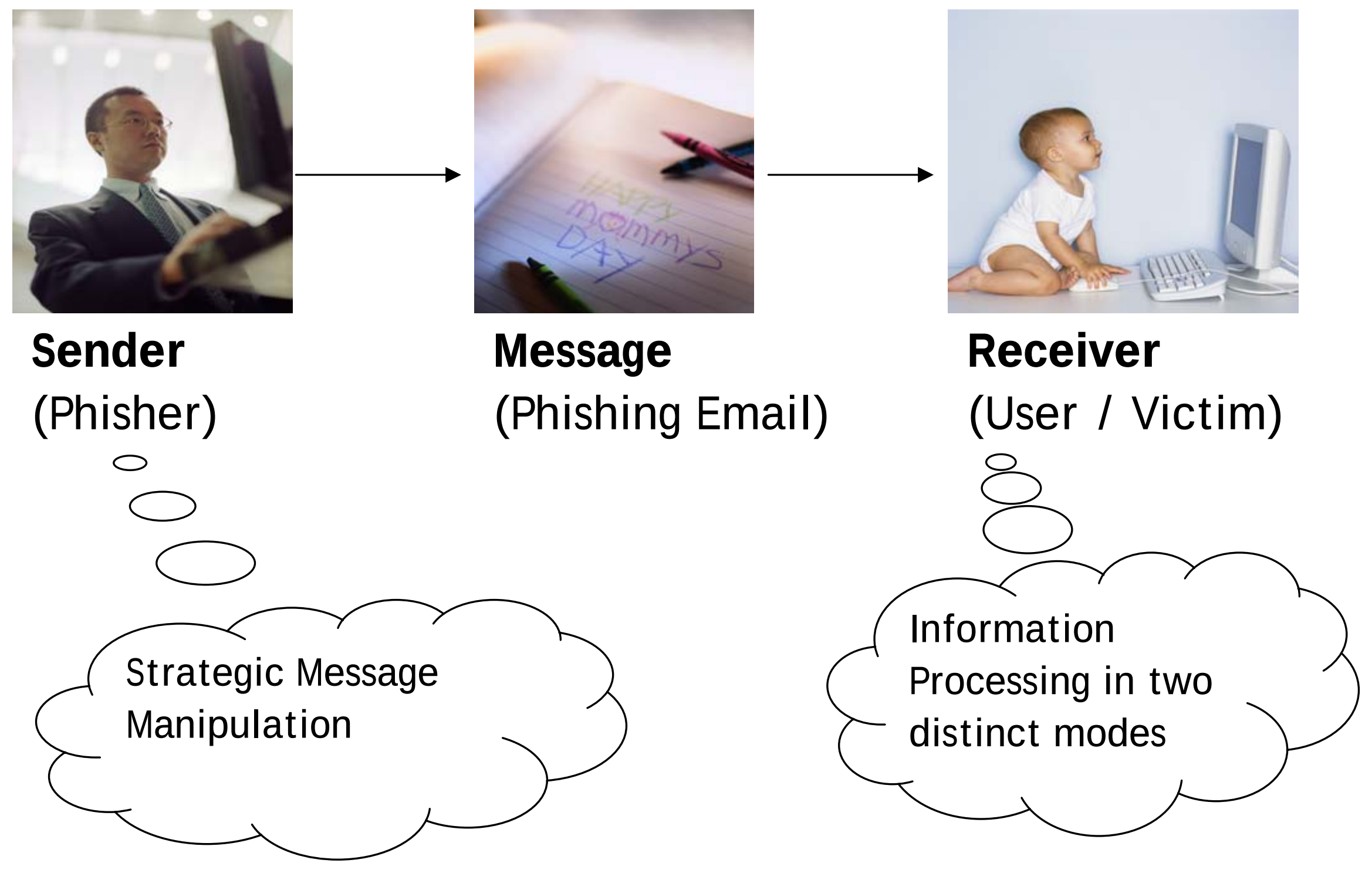
Step 4, logistic regression analysis is performed with Phishing messages & legitimate messages. The purpose of this analysis is identifying a function that can discriminate Phishing message and legitimate message.

OBJECTIVE

The objective of this paper is to present a **research framework** for phishing filter feature extraction. The framework largely consists of two parts.

- Classification of persuasive components in phishing emails—To verify if persuasive components are classified into two distinct routes of information processing
- Categorization of email messages (phishing vs no phishing) - To compute a mathematical model for binomial prediction in regards to a given message

BACKGROUND


Sender
(Phisher)

Message
(Phishing Email)

Receiver
(User / Victim)

Strategic Message Manipulation

Information Processing in two distinct modes

Theory Background

1. **SENDER**—Message Manipulation through Persuasive Transaction Components

"Phishing message can be manipulated using source, message, and channel related persuasive components."

- **Source Component**: 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).
- **Message Component**: Messages can be **rationally appealing** and/or **emotionally appealing** to message receivers message receivers are influenced by fear or guilt in relation to the message content (O'keefe, 1990; Petty & Cacioppo, 1981; Stiff & Mongeau, 2003).
- **Channel Component**: Computers can play various roles in conveying persuasive influence to the users (Fogg, 2003).
  - **Computer as a tool** aids the users in making target behavior easier.
  - **Computer as media** can appeal to users by offering vicarious experience.
  - Computers can influence users by interaction with them as if humans do, namely, **social actors.**

2. **RECEIVER**—Information Processing in Two Distinct Routes (central vs peripheral)

"Phishing email receivers process information in the message in two distinct ways."

For the analysis in this paper, we choose **Elaboration Likelihood Model (ELM, Petty & Cacioppo, 1981)**

- ELM 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.
  - **The central route—**the message recipient **attends** to the message arguments and attempts to **scrutinize** in order to evaluate them.
  - **The peripheral route-**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.

METHODS

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?

Research Steps

Our main method consists of four steps; **1) feature construction, 2) content analysis, 3) factor analysis, and 4) logistic regression analysis.** Our method consists of four major procedural steps.

- **Feature construction:** Persuasive message components are identified.
- **Content Analysis:** Based on the identified persuasive message components, we conduct content analysis of email messages.
- **Factor Analysis:** Using factor analysis, **persuasive components in phishing messages are classified for the validation of a dual process of cognition**.
- **Logistic Regression Analysis**: **Email Instances are classified by conducting logistic regression analysis.**

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

REFERENCES

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

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

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

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

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

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

PRELIMINARY RESULTS

Factor Analysis—Principal Components extraction and Varimax rotation method. Three factors were extracted and rotated. Each factor was apparently interpretable in terms of distinct characteristic; the **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.

Rotated Component Matrix			
	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.			
Rotation converged in 5 iterations.			

Logistic Regression—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.**

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 (phishing) = 18.07 + (38.39)* Email address discrepancy*
> *+ (-37.82)* Confusing destination address*

DISCUSSION & CONCLUSION

Implication & Contribution

- To text classification research by providing a framework of research method in phishing feature extraction based on information structure derived from robust communication theories.
- It is important to understand how phishing message is designed to trick people and how email users perceive manipulated messages and make trust decision.

Limitations

- Without an optimal sample size, this study only shows the research framework instead of significant research results.
- 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.
- 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.

This paper is published in "Lee, K. J. & Song, I. Y., Investigating Information Structure of Phishing Emails Based on Persuasive Communication Perspective. The ADFSL 2007 Conference on Digital Forensics, Security and Law, Arlington, VA., 2007."