COMPUTERS & SECURITY 77 (2018) 128–137

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Evaluating the applicability of the double system lens model to the analysis of phishing email judgments

Kylie A. Molinaro[a,b,*], Matthew L. Bolton[a]

[a] Department of Industrial and Systems Engineering, University at Buffalo, State University of New York, Buffalo, NY, USA

[b] Johns Hopkins University Applied Physics Laboratory, Laurel, MD, USA

ARTICLE INFO

Article history:
Received 2 December 2017
Revised 21 February 2018
Accepted 30 March 2018
Available online 5 April 2018

Keywords:
Judgment analysis
Lens model
Linear regression
Phishing
Cybersecurity

ABSTRACT

Phishing emails pose a serious threat to cybersecurity. Because human users are the last line of defense, understanding how users identify phishing emails is imperative to addressing this problem. Judgment analysis (JA) provides a means of analyzing both how information in the environment (cues) contributes to an outcome and how users synthesize cues into judgments about that outcome, typically using multiple linear regression. Because JA has not been applied to this domain, this effort assessed if the statistical assumptions of JA with multiple linear regression are upheld. We hypothesized that phishing cues are linearly combinable, meaning a lens model analysis, a type of JA, is appropriate for evaluating phishing judgments. To test this, we analyzed ten participants who judged whether or not emails were phishing using the double system lens model. Results indicated that the lens model is an appropriate means of analyzing phishing judgments, primarily evidenced by the goodness of fits for both the environment model and human judgment models. We also observed varying achievement scores across participants consistent with their varying levels of performance in the judgment task. We discuss our results and how future phishing judgment research can utilize JA afforded analysis capabilities.

1. Introduction

Phishing emails, messages designed to appear legitimate in an attempt to get individuals to reveal personal information or download malicious files, are a serious threat to cybersecurity. Phishing emails generally work by sending individuals a message with a compromised attachment or link, or include wire transfer instructions (Vishwanath et al., 2016). Successful phishing campaigns are an expensive problem, with an estimated annual impact of approximately 2.4 billion dollars (Microsoft, 2014). These expenses are associated with the theft of money, costs associated with identifying and repairing breaches, and the loss of future business. Not only are the numbers of cyber attacks increasing (Passeri, 2016; Volz, 2016), but some of the most damaging data breaches and wire transfer frauds in recent years, like those against Ubiquiti Networks Inc. and the Scoular Co. (Krebs, 2016), began with a phishing attack. The phishing problem continues to grow, with the Anti-Phishing Working Group identifying over 1.2 million separate phishing attacks in 2016, a 65% increase from 2015 (Anti-Phishing Working Group, 2017). Further, Verizon (2017) noted in their 2017 report that 95% of phishing attacks that led to a

* Corresponding author at: Department of Industrial and Systems Engineering, University at Buffalo, State University of New York, Buffalo, NY, USA.
E-mail addresses: kyliemol@buffalo.edu (K.A. Molinaro), mbolton@buffalo.edu (M.L. Bolton).
https://doi.org/10.1016/j.cose.2018.03.012
0167-4048/

breach were followed by software installation, making email attachments the most used delivery vehicle for malware.

Human users will always be the last line of defense against successful email phishing campaigns. Because of this, security groups within organizations often distribute information about how to detect phishing emails to employees. Phishing training and security notices generally focus on describing different phishing cues and where to find them in the email. However, these are not completely effective and even individuals who are informed about basic techniques for recognizing phishing emails can fall for deceptions (Caputo et al., 2014; Davinson and Sillence, 2010; Ferguson, 2005; Hong, 2012; Kumaraguru et al., 2007, 2008).

Clearly, there is a real and urgent need to understand what information humans use when making judgments about whether or not to trust an email so that phishing emails can be appropriately combated. Despite this, very little work has focused on modeling these human judgments (Pfleeger and Caputo, 2012). The work that has been done on this subject has focused on assessing susceptibility based on general individual differences (Williams et al., 2017), individual differences in cognition (Canfield et al., 2016; Vishwanath et al., 2016; Wang et al., 2012), and detection strategies (Downs et al., 2006; Zielinska et al., 2015). However, none of these analyses have focused on understanding how people use information in an email to make judgments about whether or not it constitutes a phishing attempt. The lens model is a statistical modeling judgment analysis technique that allows analysts to understand and predict how people synthesize information sources (cues) into judgments (Brunswik, 1955; Cooksey, 1996). There are a number of known cues that can help indicate if an email is a phishing attempt (Karakasiliotis et al., 2006) This suggests that the lens model would be appropriate for analyzing phishing judgments. However, it has never been used for this purpose.

The majority of lens model analyses rely on multiple linear regression (Karelaia and Hogarth, 2008; Kaufmann et al., 2013). Thus, lens model analyses work well in situations where the information provided by different cues can be linearly combined to make accurate predictions about the criteria on which judgments are being made. In this research, we attempted to evaluate whether or not the multiple linear regression assumptions of the lens model were appropriate for application to the phishing problem.

2. Background

Below we discuss the necessary background for understanding our research on the use of judgment analysis with the lens model in the phishing domain. This includes a survey of the other models that have been used to evaluate human phishing judgments, judgment analysis with the lens model, and information about the cues that appear to be important in phishing judgments.

2.1. *Human models of phishing judgment*

There is deep literature on phishing detection and filtering, however little research has focused on modeling the human user (Pfleeger and Caputo, 2012).

The suspicion, cognition, and automaticity model of phishing susceptibility (SCAM) is a cognitive-behavioral model that aims to measure individual victimization of phishing emails (Vishwanath et al., 2016). The SCAM provides a means of estimating phishing susceptibility based on several factors shown to influence overall suspicion: cyber risk-beliefs, deficient self-regulation, heuristic processing, systematic processing, and email habits. The SCAM questionnaire was administered to participants a week after the phishing email was sent. If the participant recalled the email, they answered Likert scale questions covering all previously listed factors, including overall suspicion.

Using signal detection theory to measure phishing attack vulnerability, Canfield et al. (2016) noted a greater sensitivity was positively correlated with confidence. Greater willingness to treat emails as legitimate was negatively correlated with their actions' perceived consequences and positively correlated with confidence.

Wang et al. (2012) found attention to visceral triggers, attention to phishing deception indicators, and phishing knowledge influenced phishing detection. Cognitive effort did not significantly affect detection likelihood.

Arachchilage and Love (2014) developed a theoretical model to understand how conceptual and procedural knowledge influence a user's self-efficacy against phishing attacks. Their results showed the interaction effect of conceptual and procedural knowledge positively impacted users' self-efficacy, which then enhanced their phishing threat avoidance behavior.

Other researchers have utilized a mental modeling approach. Downs et al. (2006) identified three main strategies participants used when describing their responses to emails: "(1) *this email appears to be for me*, (2) *it's normal to hear from companies you do business with*, (3) *reputable companies will send emails*." The authors noted that the awareness of phishing risks was not linked to perceived vulnerability or to useful strategies, making people more susceptible to phishing attacks. Zielinska et al. (2015) compared the mental model networks of expert and novice computer users. Results indicated experts had more links connecting phishing concepts (such as strategies for preventing phishing, trends and characteristics of phishing attacks, and the consequences of phishing) than novices.

These models help us understand different pieces of the phishing problem, but do not evaluate how a person synthesizes information in their judgments. For this, judgment analysis methods should be appropriate.

2.2. *Judgment analysis*

Judgment analysis (JA), which is based on Brunswick's probabilistic functionalism (Brunswik, 1955), is a technique for analyzing how people make judgments of distal criteria (the environment) using proximal cues (information in the environment) (Cooksey, 1996). While different statistical learning techniques can be used for this purpose (Bruins and Cooksey, 2000; Yoon et al., 2017), the vast majority of lens model analyses are based on multiple linear regression (Karelaia and Hogarth, 2008; Kaufmann et al., 2013). While there are multiple