Winter 12-13-2015

An Exploration of Phishing Information Sharing: A Heuristic-Systematic Approach

Rohit Valecha
Middle Tennessee State University

Rui Chen
Ball State University

Teju Herath
Brock University

Arun Vishwanath
University at Buffalo

Jingguo Wang
University of Texas

See next page for additional authors

Authors
Rohit Valecha, Rui Chen, Teju Herath, Arun Vishwanath, Jingguo Wang, and Raghav Rao

An Exploration of Phishing Information Sharing: A Heuristic-Systematic Approach

Rohit Valecha[1], Rui Chen[2], Teju Herath[3], Arun Vishwanath[4], Jingguo Wang[5], H. Raghav Rao[4].

{[1]Middle Tennessee State University, [2]Ball State University, [3]Brock University, [4]University at Buffalo, [5]University of Texas}

Abstract

Phishing is an attempt to acquire sensitive information from a user by malicious means. The losses due to phishing have exceeded a trillion dollars globally. Social media has provided an alternate to sharing information about phishing online. However, very little attention has been paid to phishing information sharing on social media. In this paper, we explore the risk characteristics of phishing information on social media, and investigate its effect on people's sharing of information regarding phishing. We address the research questions: (a) how do people decide which phishing information to share? (b) what aspects of phishing information are more or less consequential in influencing a user to share it? The findings suggest that the phishing messages that afford coping strategies, and come from users with higher credibility are likely to achieve higher level of sharing.

Keywords

Phishing Risk, Risk Characteristics, Information Sharing, Heuristic-Systematic Model

Introduction

Phishing is defined as "a scalable act of deception wherein impersonation is used to obtain information from a target" (Lastdrager, 2014; p. 8). Phishing involves an attacker who generally masquerades as a legitimate institution (Wang et al., 2012) to trick users into disclosing personal, financial or computer account information, and then uses this information for criminal activities such as identity theft or fraud.

In the past, information sources for reporting phishing events were limited to anti-phish services and websites, such as Millersmile[1] (Valecha et al., 2015). However, with the advent of social media, the choice of information sources reporting phishing information has broadened. Social media has allowed people to share information about a variety of issues pertaining to the phishing events, ranging from physical to personal. Social media has shown the potential for disseminating first-hand information about the phish, before it becomes available in the anti-phish services. Indeed, social media is changing the way we are creating, distributing and sharing phishing information. Yet, very little attention has been paid to how phishing information is utilized by social media users.

Acknowledging the role of social media for sharing phishing information, this study explores the characteristics of phishing messages, and examines its effects on phishing information sharing. We conceptualize "*phishing information sharing"* as the extent to which people share the phishing information by reposting it. This definition is an individual-level information processing perspective that considers how meaning is attributed to the phishing information. In this paper, we investigate how social media users share phishing information contributed by other users. We believe that the model of phishing information sharing has the potential to inform general processes of information management related to phishing. Phishing information sharing is useful first step in understanding how intentions toward phishing information are formed.

There is a vast amount of phishing information available on social media. Social media users need to devote substantial effort to searching for information that matches their needs pertaining to phishing. How do they decide which phishing information to share? Furthermore, what aspects of phishing information are more or less consequential in influencing a user to share it? To develop

[1] http://www.millersmiles.co.uk/

a theoretical framework for the research questions, we rely on the literature in the areas of information processing. This research makes two contributions: First, it suggests message framing for improving sharing of phishing information. Second, it illustrates user's reaction to phishing information. To empirically test the framework, we analyze data from Twitter social media.

The rest of the paper is organized as follows: In the next section, we introduce the literature on phishing risk and risk communication. We then develop our research model and hypotheses. Subsequently, the research methodology is introduced, and results are discussed. In closing, limitations and future research possibilities are suggested.

Background

In this section, we discuss about information sharing in social media. Then, we provide the theoretical underpinnings of a risk communication framework that is explored in this paper.

Information Sharing on Social Media

With the rapid success of social media in recent years, information sharing has received a considerable attention from academic researchers (Lee et al., 2015). The research in information sharing in social media has been categorized into two main classes: content analysis and network analysis. Content analysis has focused on the characteristics of the information in its spread. The network analysis has considered information sharing from the diffusion perspective through building an information network (Liu et al., 2012). Ha and Ahn (2011) have found that argument quality and source credibility influences the information sharing behavior. They have utilized the Heuristic-Systematic Model (HSM; Chaiken, 1980) to explain information sharing in online communities. Luo et al. (2013) argue for the use of HSM in phishing information dissemination. In a similar vein, in this paper, we employ the HSM as the basis for this study.

Heuristic-Systematic Model (HSM)

HSM was developed to examine the influence of information content and its surrounding (Chaiken et al., 1989). According to HSM, people process messages in one of two modes: systematic processing and heuristic processing. Systematic processing considers information based on its merits and comparisons to prior knowledge. Heuristic processing does not consider all the pros and cons of the message, but instead focuses on simple cues embedded in the context of the message. When using systematic processing, the recipient pays more attention to the content of the information. When using heuristic processing, the recipient depends more on heuristic cues (Chen and Chaiken, 1999). Like much previous dual-process-based research, information characteristics and source credibility are utilized in this paper to manifest the dual-process (Sussman and Siegal, 2003).

Risk Communication Characteristics

In this paper, we explore how the risk communication characteristics of the phishing message affect its sharing within the social media context.

Risk communication has been defined as "an interactive process of an exchange of information involving multiple messages about the nature of risk" (Li et al., 2014; p. 81). It has been employed to identify the underlying risk characteristics for various types of risks (Wang et al., 2015). It provides a theoretical framework that suggests that communication of risk in regard to hazards is influenced by a wide array of risk characteristics (Fischhoff et al., 1978; Slovic, 1987). Risk communication has identified three broad risk characteristics: 1) the degree to which a risk is known, 2) the degree to which a risk evokes the feeling of dread, and 3) the degree to which a risk can be controlled (Slovic et al., 1980; Slovic et al., 1987). In the next section, we discuss our research model, and develop testable hypotheses.

Hypothesis Development

Drawing on the heuristic-systematic model and the risk communication model, we propose a research model (see Figure 1) relating the extent to which phishing risk characteristics predict phishing information sharing.

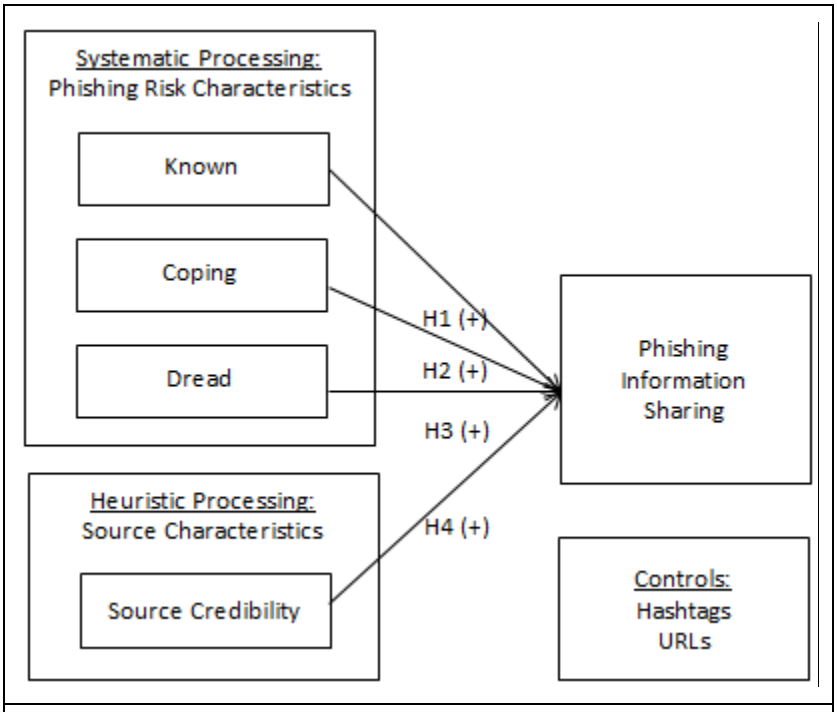

Figure 1. Research Model

Effect of Phishing Risk Characteristics on Phishing Information Sharing

When the users of social media assess the validity of the information in a message related to phishing, they engage in systematic processing of information. When these users carefully read the message and contemplate its validity, they are engaging in the systematic route of information processing. Phishers employ a variety of techniques to trick potential victims to obtain access to their information (Lastdrager, 2014). When a message provides knowledge about a phish or a phishing technique, it allows users to reduce uncertainty related to it. This knowledge also builds

users' confidence, and improves their competency to evaluate and comprehend phishing information (Lion et al., 2002). Thus the messages that convey knowledge about the phish are likely to result in higher information sharing.

H1: Messages that provide knowledge about the phish are likely to produce a higher level of information sharing

In the same vein, if a message affords strategies to cope with a phish, it helps users gain the feeling of control, and to avoid potential grave negative consequences (Neuwirth et al., 2000). The coping strategies also enable users to improve their response efficacy and self-efficacy (Herath et al., 2014), which enables them to take effective coping actions against the threat (Wang et al., 2015). Thus the messages that suggest strategies to counter the phish are likely to result in higher information sharing.

H2: Messages that afford strategies to cope with the phish are likely to produce a higher level of information sharing

The existing literature on emotions has shown that dread might trigger a high level of physiological arousal (Berger, 2011). This physiological arousal has been shown to be more viral (Stieglitz and Dang-Xuan, 2013). The content that evokes physiological arousal is a driver of information sharing (Berger and Milkman, 2012). This also explains why the news agencies often report negative and fearful news to capture audiences (Li and Rao, 2014). The rumor literature has also argued that messages high in dread, get disseminated faster (Oh et al., 2013). The above arguments lead us to hypothesize:

H3: Messages that are characterized by dread related to the phish are likely to produce a higher level of information sharing

Effect of Source Characteristics on Phishing Information Sharing

In social media, there is a vast amount of information that a user needs to process. Social media users receive large numbers of messages from their friends or those they follow. Often, this causes information overload. To curb information overload, social media users often use heuristic cues (Vishwanath et al., 2011), such as source credibility, as a means to quickly evaluate the message. Social media technologies present a rich set of features that can serve as heuristic cues. Research also indicates that individuals following the heuristic route can be influenced by the source's attractiveness, likeability, and credibility (Sussman and Siegal, 2003). Other examples include information about the author of the message, the number of friends or followers, number of activities etc. Heuristic cue processing based on source credibility tends to complement systematic processing, and tends to influence assessment of the message (Zhang and Watts, 2008), which leads us to hypothesize the following:

> H4: Messages posted by users that have higher source credibility are likely to produce a higher level of information sharing

Studies have also shown that there are a number of other factors that also have an impact on information sharing behavior in social media, such as inclusion of hashtags and inclusion of URLs (Stieglitz and Dang-Xuan, 2013). Therefore, we include these variables as controls.

Methodology

In this section, first we discuss the data collection methodology in detail. Next, we define our coding scheme and coding reliability. Finally, we present details on the descriptive statistics and analysis technique.

Data Collection

For this research, we collected tweets from Twitter microblog through the streaming APIs using the keyword #phishing, #vishing, #phished, #vished and #phishingmails for 33 days starting from June 14, 2014 and ending on July 17, 2014.

Coding Scheme

We used the retweet count for the tweet message as the measure of dependent variable, information sharing. Following examples from Zhang and Watts (2008), the variable source credibility was measured as log of follower counts of the message sender. Then, we coded each tweet message for the variables known, coping and dread. The control variables hashtags and URL were coded based on the presence of hashtags and URLs respectively. Table 1 details the coding scheme for the risk characteristics. All the risk characteristics were coded as dichotomous (either 1 or 0) in the content analytic coding procedure used.

Table 1. Coding Scheme

Variable	**Definition**	**Coding**	**Example**
Known: Based on Wang et al. (2015)	A message indicating presence of a phish	1 = Phish 0 = No phish	#iPhone Beware iPhone Phishing Scams in Wake of iOS Lockouts
Coping: Based on Slovic (1987)	A message indicating coping mechanisms to control phish	1 = Specify coping mechanisms 0 = Does not specify coping mechanisms	How to recognize #phishing #email messages? Issued in Public interest by Tech Squad Today just call @1-855-704-1390
Dread: Based on Slovic (1987)	A message expressing fear due to phish victimization	1 = Indicate Victimization 0 = No victimization	Were you one of the 145M users compromised in the #eBayhack?

Inter-coder Reliability

We followed the steps for content coding and analysis suggested by Krippendorf (1980) and Landis and Koch (1977). For the content coding, four Master's students were hired to separately code the Twitter data. Pilot data coding was carried out in two rounds for the data set. For the first pilot coding, we used 65 tweet samples that we randomly selected from our original data set. The first pilot coding resulted in a kappa value of .63. The coders then performed coding with another 65 sample tweets. This final pilot coding resulted in a kappa value of .80, thereby confirming that our coding is robust. Each graduate student coder then proceeded to separately code the tweet data sample. The pilot sample data were excluded from the data sample.

Descriptive Statistics

The sample size is 1458 tweets, out of which 811 tweets are retweets, and another 647 are unique tweet messages. The Spearman rank correlation test indicates that all correlations are less than 0.5, indicating that no significant multicollinearity problems exist (Kishore et al. 2004). The descriptive statistics and correlations are shown in Table 2.

Table 2. Data Descriptive and Correlation (See legend below)

N=647	Mean	S.D.	Freq.	1	2	3	4	5	6	7
1	2.253	26.629		1						
2			30.6%	0.08*	1					
3			50.4%	0.17**	0.31**	1				
4	2.468	1.052		0.35**	0.16**	0.25**	1			
5			18.9%	0.03	-0.01	-0.03	-0.08*	1		
6			16.1%	-0.07	-0.01	-0.15**	-0.08	-0.13**	1	
7			25.3%	0.08*	0.14*	0.34**	0.09*	-0.10*	0.03	1

Legend – 1: Retweets; 2: Hashtags; 3: URL; 4: Source Credibility; 5: Coping; 6: Dread; 7: Known

* p < 0.05; ** p < 0.01; *** p < 0.001

Analysis

In order to examine the effect of phishing risk characteristics on phishing information sharing, we ran zero-inflated negative binomial regression using pscl package in R statistical software. When the dependent variable is a count variable, as in our case of retweet counts, Ordinary Least Square (OLS) regression cannot estimate the appropriate statistics because of violation of normality in residuals. Negative binomial regression has been suggested as a possible method to deal with count dependent variables (Osgood, 2000). However, since the retweet counts are over-dispersed and zero-inflated, the model was tested using zero-inflated negative binomial regression as follows:

$$Log(Retweets) = \beta_0 + \beta_1 Hashtags + \beta_2 URL + \beta_3 Source\ Credibility + \beta_4 Known + \beta_5 Coping + \beta_6 Dread + e$$

Results

Using zero-inflated negative binomial regression, we estimated the effects of phishing risk characteristics, such as known, coping and dread, on the phishing information sharing. The result of the regression analysis is summarized in Table 3. Vuong-test[2] indicates that the model has a good fit to the data, AIC-corrected z-statistic = -6.481, p < 0.001.

The results show significant positive effects of risk coping on phishing information sharing, at p < 0.05, leading to support for hypothesis H2. This implies that tweet messages that afford strategies to cope with the phish are more than thrice (3.300 times) as likely to produce a higher level of

[2] Vuong-test (Vuong, 1989) compares the predictor model (alternate model) with the null model (intercept-only model). Vuong test-statistic (z-statistic) is asymptotically distributed N(0,1) under the null hypothesis that the models are indistinguishable.

information sharing. The effect of phishing risk dread on phishing information sharing is also significant but negative at $p < 0.001$. Thus, hypothesis H3 is rejected. Also, different from our expectation, we could not find significant effect of phishing risk knowledge on phishing information sharing. Therefore H1 is rejected. Furthermore, the results also show significant positive effects of source credibility on phishing information sharing at $p < 0.001$. In other words, the tweet messages posted by users that have higher source credibility are 6.423 times more likely to produce a higher level of information sharing.

Table 3. Results of Zero-Inflated Negative Binomial

	Estimate	**Std. Err.**	**Z Value**	**Exp(β)**	**Hypothesis**
Intercept	-5.637	0.577	-9.762	0.004***	
Hashtag	0.513	0.390	1.315	1.670	
URL	-1.415	0.351	-4.037	0.243***	
Known	0.525	0.385	1.362	1.690	H1 Not Supported
Coping	1.194	0.387	3.084	3.300**	H2 Supported
Dread	-2.052	0.590	-3.475	0.128***	H3 Not Supported
Source Credibility	1.860	0.168	11.085	6.423***	H4 Supported

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Discussion

The result of overall zero-inflated negative binomial regression indicates that messages that afford coping strategies, and come from the users with higher credibility are likely to be shared more. When dealing with phishing risk, people are more eager to share coping messages.

As a theoretical contribution, we extend heuristic-systematic model to incorporate risk characteristics in order to examine the effect on phishing information sharing in social media. By

doing so, we introduce a novel angle to investigate phishing information sharing. As phishing threats pose varied levels of risk to users, it is important for researchers to investigate the risk characteristics when examining users' behaviors on social media. The findings of this study reveal interesting patterns of risk characteristics within messages from the total population, influential users and popular users.

From a practical standpoint, our study suggests that organizations could design risk communication messages to communicate about various phishing attacks. Within risk communication, coping is an important strategy to engage users in responsible security behaviors (Wang et al., 2015). The risk communication messages should be properly framed with the considerations to risk characteristics to alter users' risk attitudes toward phishing, and motivate coping behaviors.

Conclusion

Recently, phishing attacks have caused significant losses to individuals, organizations and economies globally with losses exceeding a trillion dollars. Social media has provided an alternate to sharing first-hand information about phishing to substantial population at a rapid rate in a short span of time. In this paper, we explore phishing information sharing on social media, in relation to the phishing risk characteristics, namely known, coping and dread.

The findings suggest that the messages for phishing information sharing should be high on coping, and come from credible sources. This study has the following limitation. We coded contextual variables in binary data form; there could be information loss during coding and analysis. It was, however, an inevitable choice since coders manually read and coded all data of tweet texts. One future direction for this work would be to incorporate additional risk characteristics such as

preventable, mitigatable, observable, old (or new), and immediacy into the model. Another future work[3] would be to investigate whether two-way and even three-way interactions can be modeled, for example, the interaction of source credibility and risk characteristics (coping). Such an interaction effect can further enhance the sharing of a phishing risk message. Furthermore, when the users of social media assess the validity of the information in a message related to phishing, they engage can engage in systematic information processing or heuristic information processing or a combined approach. We leave that investigation for the future[4] studies.

Acknowledgements

The authors would like to thank the reviewers for their critical comments that have greatly improved the paper. This research is supported in part by NSF Grant No. 1241709, 1554373 and 1227353. Usual disclaimer applies.

References

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. Journal of personality and social psychology, 39(5), 752.

Chaiken, S., Liberman, A., and Eagly, A. H. (1989). Heuristic and Systematic Information Processing within and Beyond the Persuasion Context, in J. S. Uleman and J. A. Bargh (Eds.) Unintended Thought, New York: Gilford Press, pp. 212-252.

Chen, S., and Chaiken, S. (1999). The heuristic-systematic model in its broader context. Dual-process theories in social psychology, 73-96.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., and Combs, B. (1978). How Safe Is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits. Policy Sciences (9:2), pp. 127-152.

Ha, S., and Ahn, J. (2011). Why are you sharing others' tweets?: The impact of argument quality and source credibility on information sharing behavior. In Proceedings of ICIS 2011.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. (2014). Security services as controlling mechanisms: an investigation into user intention to adopt an email authentication service. Information Systems Journal 24(1) 61-84.

Joyce, E., and Kraut, R. (2006). Predicting continued participation in newsgroups. Journal of Computer-Mediated Communication, 11, 3 (2006), 723–747.

Kishore, R., Agrawal, M., and Rao, H. R. (2004). Determinants of sourcing during technology growth and maturity: An empirical study of e-commerce sourcing. JMIS, 21(3), 47-82.

[3] We thank the anonymous reviewers for this suggestion.

[4] We thank the anonymous reviewers for this suggestion.

Krippendorff, K. (2012). Content analysis: An introduction to its methodology. Sage.

Landis, J. R., and Koch, G. G. (1977). The Measurement of Observer Agreement for Categorical Data. Biometrics (33), pp. 159-174.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, 3(1), 1-10.

Lee, J., Agrawal, M., and Rao, H. R. (2015). Message diffusion through social network service: The case of rumor and non-rumor related tweets during Boston bombing 2013. Information Systems Frontiers 17(5): 997-1005

Li, J., Vishwanath, A., and Rao, H. R. (2014). Retweeting the Fukushima nuclear radiation disaster. Communications of the ACM, 57(1), 78-85.

Lion, R., Meertens, R. M., and Bot, I. (2002). Priorities in Information Desire About Unknown Risks. Risk Analysis (22:4), pp. 765-776.

Liu, Z., Liu, L., and Li, H. (2012). Determinants of information retweeting in microblogging. Internet Research, 22(4), 443-466.

Luo, X. R., Zhang, W., Burd, S., and Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. Computers and Security, 38, 28-38.

Neuwirth, K., Dunwoody, S., and Griffin, R. J. (2000). Protection Motivation and Risk Communication. Risk Analysis (20:5), pp. 721-734.

Oh, O., Agrawal, M., and Rao, H. R. (2013). Community intelligence and social media services: a rumor theoretic analysis of tweets during social crises. MIS Quarterly, 37(2), 407-426.

Slovic, P. (1987). Perception of Risk. Science (236:4700), pp. 280-285.

Slovic, P. (2000). The Perception of Risk. Sterling, VA: Earthscan.

Slovic, P., Fischhoff, B., and Lichtenstein, S. (1980). Facts and Fears: Understanding Perceived Risk. In Societal Risk Assessment: How Safe Is Safe Enough?, R. Schwing and W.A. Albers, Jr., (eds.). New York, pp. 181-216.

Slovic, P., MacGregor, D. G., and Kraus, N. N. (1987). Perception of Risk from Automobile Safety Defects. Accident Analysis and Prevention (19:5), pp. 359-373.

Stieglitz, S., and Dang-Xuan, L. (2013). Emotions and information diffusion in social media—Sentiment of microblogs and sharing behavior. Journal of Management Information Systems, 29(4), 217-248.

Sussman, S. W., and Siegal, W. S. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. Information systems research, 14(1), 47-65.

Ungar, S. (1998). Hot crises and media reassurance: A comparison of emerging diseases and Ebola Zaire. The British Journal of Sociology 49, 1 (Mar. 1998), 36–56.

Valecha, R., Chen, R., Herath, T., Vishwanath, A., Wang, J., and Rao, H. R. (2015). An Exploration of Language Acts of Persuasion in Phishing Emails. In The 2015 Dewald Roode Workshop on Information Systems Security Research.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586.

Vuong, Q. (1989). Likelihood ratio tests for model selection and non-nested hypotheses. Econometrica 57, 307-334.

Wang, J., Chen, R., Herath, T., Vishwanath, A., and Rao, H. R. (2012). Phishing Susceptibility: An Investigation into the Processing of Targeted Spear Phishing Email. IEEE Transactions on Professional Communication 55(4) 345-362.

Wang, J., Xiao, N., and Rao, H. R. (2015). An exploration of risk characteristics of information security threats and related public information search behavior. Information Systems Research.

Zhang, W., and Watts, S. A. (2008). Capitalizing on content: Information adoption in two online communities. Journal of the Association for Information Systems, 9(2), 3.