Winter 12-13-2015

The Role of Trust and Familiarity in Click-through Intention: A Perception Transfer Theory in a Cybersecurity Context

Obi Ogbanufe
University of North Texas

Dan Kim
University of North Texas

The Role of Trust and Familiarity in Click-through Intention: A Perception Transfer Theory in a Cybersecurity Context

Research in Progress

Obi Ogbanufe

University of North Texas, Denton, Texas, USA {obi.ogbanufe@unt.edu)

Dan J. Kim

University of North Texas, Denton, Texas, USA {DanKim@unt.edu)

ABSTRACT

Despite constant reminders, warnings on avoidance techniques, information security policies, and anti-virus software reminders, individuals still fall prey to malware attacks. This paper looks at the role that familiarity and trust play on the individual's intention to click-through web based malware. Hypotheses are developed to suggest that click-through intention is influenced by trust and familiarity. Two scenarios to test the hypotheses are described. Expected contributions and limitations are noted.

Keywords: trust, trust transfer, familiarity, malware, information security, click-through

INTRODUCTION

Identified as the second most organizational and management issue in 2014 (Kappelman et al. 2014), information security (IS) and cybersecurity concerns have risen in its ranking in both organizational and national levels. Among the threats to cybersecurity, malware attacks rank highest (Computer Security Institute 2011) and are used by criminals to steal personal information or access networks, thus resulting in significant productivity and financial losses to individuals and organizations (Stafford and Urbaczewski 2004). Malware has evolved to web-based malware which are more sophisticated and difficult to detect. Attackers often use compromised but legitimate websites to distribute malware, making it difficult for users to detect

and security administrators to remove. Users are also known to click-through to malware websites, even after being warned by their internet browsers of the website's potentially infections nature (Almuhimedi et al. 2014). The financial impact of computer crimes like these is estimated at over one trillion dollars each year worldwide. Many studies on IS have focused on organization policies – its violation and compliance, neglecting some of the dynamic nature of the security risks and threats individuals face. However, given the uncertainty in IS findings on deterrence and compliance policies (D'Arcy and Herath 2011) and the immensity of attacks and imminent threats posed by malware, it is important to examine other factors affecting users' behavioral intention towards cybersecurity threats. We do so by examining the issue of malware through different lenses. Based on trust and trust transfer theory we argue that malware click through intention is influenced by (1) familiarity and (2) trust transferred from a source site to a target site. Thus, this study seeks to address the gap by attempting to answer the following research questions. (1) How do familiarity and trust affect the individual's intention to click-through a malware website? (2) How does trust transfer from one website to another influence the users' click-through intention? We argue that malware click-through intention is influenced by familiarity and trust transferred from a source site to a target site. Also important in this study is the examination of the intersection between trust based attitude towards e-commerce and trust based attitude towards security. We expect to show the similarities between intention in an e-commerce context and intention in a web based malware context. We hope this study expands our understanding of this phenomenon, and helps practitioners device more effective avoidance and defensive strategies for web-based malware.

LITERATURE REVIEW

An individual is infected with web-based malware when their browser is exposed to malicious content, which happens when the individual visits malicious websites or clicks through malicious

URLs on legitimate sites. In their 4 months study to examine user behavior towards malware, Lalonde Levesque et al. (2013) found that 38% of their sample were exposed to malware. Indicative that malware exposure is inevitable for internet users. This is especially relevant to practitioners and organizations, such that while it informs them of the universal susceptibility users face using the internet, it also provides an alternative view of their IS countermeasures, encouraging a balance between promoting secure user behavior and technologies/risk management policies that include user participation (Spears and Barki 2010). Studies using compliance theories, protection motivation theories, and deterrence theories (e.g. Johnston and Warkentin 2010; Vance et al 2012) provide explanations for promoting secure behavior, and deterring wrong behavior. However, the gap that exists is that IS risks faced by individuals are dynamic and increasingly sophisticated, such that current studies have provided limited explanations, and few studies addressed. As the gap between controls (e.g. policies, technologies) and security vulnerabilities continue to grow, cybercriminals will exploit undiscovered holes in applications and networks.

THEORETICAL BACKGROUND

Early trust transfer literature argue that trust can develop through a transference process. It has been described as a pattern of trust extension (Doney and Cannon 1997; Strub and Priest 1976), using another party's definition of another as a basis for defining that other as trustworthy. This suggests that trust can be transferred from one source to another, where the trustor has little of no direct experience with the 'another' (Milliman and Fugate 1988). Trust transfer theory posits that an individual's perceptions towards an object is transferred from perceptions of other reference objects associated with the target object or from different sources (Stewart and Zhang 2003). In this study, trust transfer theory is used to explain the effect of trust transferred from a source site to another site (target) and consequently on an individual's intention to click-through web-based

malware. A number of studies have empirically offered support for trust transfer in both offline and online settings. For example, Doney and Cannon (1997) and Milliman and Fugate (1988) found that the process of transference predicted a positive relationship. Trust transfer and familiarity offer an explanation for why individuals click-through potential malware URLs even when they are aware of the risks. Figure 1 depicts the research model with constructs of interest in this study. In this model, trust is assumed to affect intention directly, and also indirectly through a mediator, trust of target site.

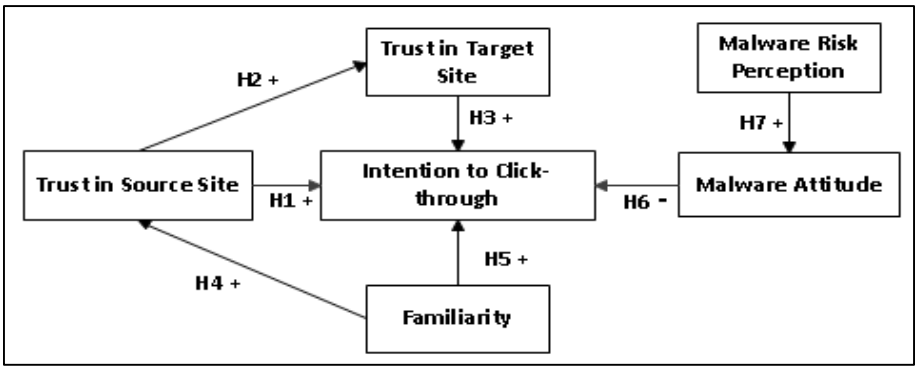

Figure 1: Research Model

Hypotheses Development

Trust

The context of this study is one where individuals having established a level of trust with an online site (e.g. Amazon.com, search engine), and with feelings of less inhibition, click on any link on the website in order to transact business. Building on earlier trust definitions and the context of this study, we define trust in source site as the *expectation that the site owner's site and links are dependable* (Gefen 2000). We expect that individuals assured of a site owner, will develop a reduced notion of uncertainty, and click on links displayed on the website. We also test the transfer of trust from one site to another, and whether this transfer affects the individual's intention to click-through. The trust transfer theory is used to explain the effect of trust transferred from a source site to another site (i.e. target site) and also on an individual's

behavioral intention. Thus, we define trust in target site as *the individual's belief that the target site links are dependable by virtue of its association with the source site*. Lim et al. (2006) found that an affiliation with a well-known portal will improve potential customers' trusting beliefs of an unfamiliar online store. We expect that trust in a source site will influence the individuals' intention to click-through links on the website (i.e. the direct effect of trust), and that the transfer of trust from source to target site (i.e. the indirect effect of trust) will affect the individual's behavioral intention to click-through to a target website.

H1: Trust in source site positively influences intention to click-through
H2: Trust in source site positively influences trust in target site
H3: Trust in target site positively influences intention to click-through

Familiarity

Familiarity refers to one's understanding of another's behavior based on prior interactions or experiences (Bhattacherjee 2002). Omitted in most cybersecurity studies, the effects of familiarity in e-commerce context is viewed in this study as analogous to a cybersecurity context. For example, individuals who have developed a favorable understanding of an e-commerce site and as a result estimated the likelihood of desired future favorable behavior (Bhattacherjee 2002; Gefen 2000) will form a relationship with this site. This relationship tends to reduce the uncertainties the individual may have, and influence the individuals' trust in the site owner. Familiarity is also expected to influence intention to click-through. Similarly, in a cybersecurity context, an individual who is familiar through previous interactions with a source site will tend to trust the site, and click-through links on the website. Consistent with previous studies that tested the relationship between familiarity, trust and intention (Bhattacherjee 2002; Gefen 2000; Kim et al. 2009) we hypothesize:

H4: Familiarity positively influences trust in source site
H5: Familiarity positively influences intention to click-through

Malware Attitude

Malware attitude is defined as an individual's negative affect towards malware, and intention is defined as the individual's willingness to click-through a malware URL. Theory of planned behavior (TPB) (Ajzen 1991) and theory of reasoned action (TRA) (Fishbein and Ajzen 1975) postulate that an individual's attitude predicts their behavioral intention and that behavioral intention determines whether the individual will perform a certain behavior. Given an individual's negative malware attitude, we expect a negative relationship towards malware click-through. Therefore, we hypothesize:

H6: Malware attitude negatively influences intention to click-through

Malware Risk Perception

According to risk theory, the presence of risks will result in risk-averse tendencies in individuals (Sitkin and Pablo 1992). Malware risk perception is defined as the individual's assessment of a risky situation. A persons' subjective perception of the risk of malware infection will influence their attitude towards malware. Malware involves the potential disruption of normal operations of computing devices, thus we expect that as the individual's perception of malware risk increases, it also increases their negative malware attitude. Risk perception has been studied in different situations with results consistently showing that risk perceptions influenced attitudes and behavior (Chen et al. 2011; Dillard et al. 2012). Therefore, we hypothesize:

H7: Malware risk perception positively influences malware attitude

METHODOLOGY

This study developed two scenarios and questionnaires. The first scenario utilized Amazon.com (A) and the second, used search engine (B) as the source sites. In each scenario, respondents are asked to assume purchasing a gift for a friend, and searching for this gift through the source site. In scenario A, the search result page shows the item as being sold only by an Amazon seller,

with a link on the product information indicating the respondent click-through to the seller's website in order to purchase the product. In scenario B, the search result includes several hits, one of which has a good price. Questionnaires are designed and administered to assess the subsequent behavioral intention of individuals - in each scenario - towards clicking through to the target site to purchase the gift item. Given that Amazon has been heavily used in several trust and intention studies (Gefen 2000; Pavlou 2003), we propose using two scenarios to access whether click-through intentions differ on the basis of trust of the source sites and malware attitude.

DISCUSSION AND CONCLUSION

We expect to show that trust and familiarity are significant determinants affecting the individual's intention to click-through web-based malware sites. This study's contribution is in the extension of the theory of trust and trust transfer in e-commerce (Gefen 2000; Luhmann 2000) to cybersecurity. We seek to provide new insights to how and why individuals fall prey to web-based malware irrespective of risks, warnings, compliance, and deterrence. This research has a limitation in the use of convenience sampling of university students. The findings from this research will have important practical implications, helping practitioners understand web-based malware in a similar light as e-commerce, and therefore devising means to educate and curtail attacks from web-based malware.

REFERENCES

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.

Almuhimedi, H., Felt, A. P., Reeder, R. W., and Consolvo, S. 2014. "Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning," *Symposium on Usable Privacy and Security (SOUPS)*.

Bhattacherjee, A. 2002. "Individual Trust in Online Firms: Scale Development and Initial Test," *Journal of management information systems* (19:1), pp. 211-241.

Chen, R., Wang, J., Herath, T., and Rao, H. R. 2011. "An Investigation of Email Processing from a Risky Decision Making Perspective," *Decision Support Systems* (52:1), pp. 73-81.

Computer Security Institute. 2011. "Computer Crime and Security Survey." from http://analytics.informationweek.com/abstract/21/7377/Security/research-2010-2011-csisurvey.html

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

Dillard, A. J., Ferrer, R. A., Ubel, P. A., and Fagerlin, A. 2012. "Risk Perception Measures' Associations with Behavior Intentions, Affect, and Cognition Following Colon Cancer Screening Messages," *Health psychology* (31:1), p. 106.

Doney, P. M., and Cannon, J. P. 1997. "An Examination of the Nature of Trust in Buyer-Seller Relationships," *the Journal of Marketing*), pp. 35-51.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Gefen, D. 2000. "E-Commerce: The Role of Familiarity and Trust," *Omega* (28:6), pp. 725-737.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-A544.

Kappelman, L., McLean, E., Johnson, V., and Gerhart, N. 2014. "The 2014 Sim It Key Issues and Trends Study: Appendix," *MIS QUARTERLY EXECUTIVE* (13:4).

Kim, D. J., Ferrin, D. L., and Rao, H. R. 2009. "Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration," *Information Systems Research* (20:2), pp. 237-257.

Lalonde Levesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., and Somayaji, A. 2013. "A Clinical Study of Risk Factors Related to Malware Infections," *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*: ACM, pp. 97-108.

Luhmann, N. 2000. "Familiarity, Confidence, Trust: Problems and Alternatives," *Trust: Making and breaking cooperative relations* (6), pp. 94-107.

Milliman, R. E., and Fugate, D. L. 1988. "Using Trust-Transference as a Persuasion Technique: An Empirical Field Investigation," *Journal of personal selling & sales management* (8:2), pp. 1-7.

Pavlou, P. A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International journal of electronic commerce* (7:3), pp. 101-134.

Sitkin, S. B., and Pablo, A. L. 1992. "Reconceptualizing the Determinants of Risk Behavior," *Academy of management review* (17:1), pp. 9-38.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-A505.

Stafford, T. F., and Urbaczewski, A. 2004. "Spyware: The Ghost in the Machine," *The Communications of the Association for Information Systems* (14:1), p. 49.

Stewart, K. J., and Zhang, Y. 2003. "Effects of Hypertext Links on Trust Transfer," *Proceedings of the 5th international conference on Electronic commerce*: ACM, pp. 235-239.

Strub, P. J., and Priest, T. 1976. "Two Patterns of Establishing Trust: The Marijuana User," *Sociological Focus* (9:4), pp. 399-411.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3–4), pp. 190-198.