WISP 2016 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-10-2016

Going Through the “Emotions”: Identity Protective Responses

Obi Ogbanufe
University of North Texas, obi.ogbanufe@unt.edu

Robert Pavur
University of North Texas, robert.pavur@unt.edu

Going Through the "Emotions": Identity Protective Responses

Research-in-Progress

Obi Ogbanufe
University of North Texas, Denton, TX 76201, USA. {Obi.Ogbanufe@unt.edu}

Robert Pavur
University of North Texas, Denton, TX 76201, USA. {Robert.Pavur@unt.edu}

ABSTRACT

This study examines identity theft, specifically, the mechanisms through which individuals protect themselves using credit monitoring information. As an adaptive protective response against identity theft, we conceptualize credit monitoring information as an information product. By integrating protection motivation theory with the extended parallel process model, we seek to understand how individuals either take adaptive recommended actions or maladaptive ones. A research model, hypotheses, and an experiment are described.

Keywords: identity theft, credit monitoring, data breach, extended parallel process model

INTRODUCTION

In recent years, security breaches (e.g. Target, Home Depot, Anthem) involving the exposure of several millions of individuals' personally identifiable information (PII) fill the news. Individuals face great financial and psychological risks from security breaches that result in identity theft (Sharp et al. 2004). According to Javelin (2015), in 2105 more than 13.1 million adults in the U.S became victims of identity theft (IDT) and lost a total of $15 billion to thieves. With identity related theft activities at the forefront of Federal Trade Commission's (FTC) consumer complaint in 15 consecutive years (FTC 2015), there is a need to understand how individuals cope with and respond to these issues using information systems. IDT refers to the misuse of another person's personal information to commit fraud (Gonzales and Majoras 2007). While IDT has become a focus for regulators, organizations and individuals, there is scant empirical and theoretical based research in this area (Hemphill 2001; Milne 2003), especially as it relates to individuals' financial and personal well-being. Hence, this study focuses on how individuals protect themselves using credit monitoring information (CMI). The following research question is identified, *what are the effects of identity theft on the individual's motivation to adopt credit monitoring information protection*? We propose a model that integrates both protection motivation theory (PMT) and extended parallel process model (EPPM) to explain the process through which individuals either take an adaptive coping response or a maladaptive coping response. The combination portrays a nuanced picture anchored on the importance of studying how and why individuals take protective mechanisms to protect against IDT, choose to do nothing, or reject the message outright. By including financial well-being as a personal relevance construct (Johnston et al. 2015) specific to the IDT, we extend PMT in information security research. For practice, in highlighting these alternate paths, we explicate factors contributing to maladaptive response and how organization's users can be trained to accept future messages.

THEORETICAL BACKGROUND

The individual's identity can be a combination or a subset of PII that includes but is not limited to the individual's name, social security number, driver's license, financial account numbers (FTC 2015), and tightly linked to both the person's financial history and future. It is the form of identity needed in order to secure a home mortgage or employment. Identity theft can occur offline and online (Lai et al. 2012). Prior IDT research include its effect on payment systems (Kahn and Liñares-Zegarra 2015), IDT cycle (Albrecht et al. 2011), and fear of identity theft (Roberts et al. 2013). As a step to mitigate the threat of IDT or reduce the impact, it is a generally accepted notion that a quick discovery of the theft limits the attendant damages (Anderson 2005). This quick discovery is usually accomplished with credit monitoring information. Credit monitoring utilizes an information system to regularly monitor a person's financial information against fraudulent activities, and assists in reconciling and cleaning questionable transactions (Johnson 2011). Credit monitoring information is a protective measure against economic harm due to identity theft (Johnson 2011). Following Raghunathan and Sarkar (2016), we conceptualize credit monitoring as an information product. The primary objective of consumers of an information product is to "obtain a reliable estimate of some quantity of interest that will help her make a sound decision" (p. 111). Similarly, in our case, the consumer's objective is to receive information regarding suspicious financial activities, in order to help resolve the issue. We define the individual's intention to use CMI as a protective behavior that individuals voluntarily engage for protecting against IDT. PMT suggests that individuals facing a threat will appraise the threat through their perceptions of severity of and their vulnerability to the threat. In addition, individuals appraise the effectiveness of a coping response (Maddux and Rogers 1983; Rogers 1975). PMT's criticisms is that it does not specify when and why people reject adaptive recommendations (Witte 1998). The EPPM (Witte 1992) addresses the limitations of PMT by distinguishing the aspects of a stimulus that bring about the cognitive (danger control) from the aspects that bring about the emotional (fear control). EPPM posits that perceived efficacy (self-efficacy and response efficacy) is the determinant of whether it is danger control or fear control that is initiated, and perceived threat (severity and vulnerability) is the determinant of the intensity of the responses (Witte 1992). The EPPM puts the focus back on the effect of the emotion, fear. According to Witte (1992; 1994), the manipulation of perceived efficacy activates the fear control (emotional affect based) processes and results in maladaptive response. When individuals are presented with high threat but presented with low efficacy solution to the threat, the user may feel that there is little chance that the solution (response efficacy) will mitigate the threat. Thus, the user enacts maladaptive responses, denial, avoidance, rejection etc. In order to represent both adaptive and maladaptive as separate and distinct responses to fear appeal, the proposed model (Figure 1) integrates PMT (dashed line) and EPPM. This study incorporates both message acceptance that leads to adaptive responses, and message rejection that leads to maladaptive responses in order to fully understand the effect of fear appeals in persuading and motivating individuals in InfoSec. Perceived threat (severity and vulnerability), perceived efficacy (response efficacy and self-efficacy), and perceived financial well-being affect CMI. We conceptualize intention to use CMI as the danger control and cognitive aspect of adaptive response. On the lower right side of the model is the integration of the EPPM. Avoidance and denial are jointly conceptualized as the maladaptive response (Witte 1994).

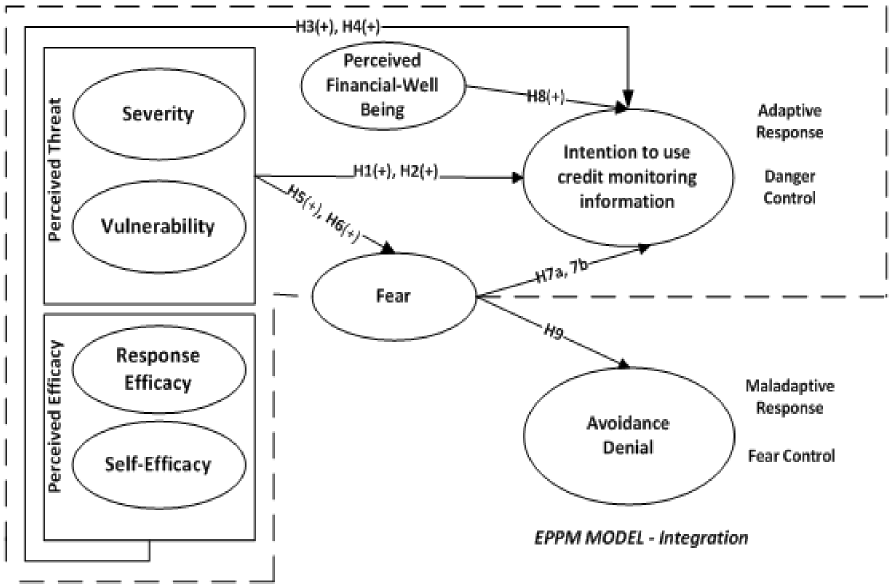

Figure 1: Research Model

HYPOTHESES DEVELOPMENT

Danger Control

Threat appraisal includes severity and vulnerability of threat. Severity is the degree to which individuals see the consequences of being an IDT victim as severe (i.e., how severe the damage caused by identity theft will be). Vulnerability is the probability that the individual will be an IDT victim. Severity of IDT can be the loss of income, denial of credit for home or car purchase, the out-of-pocket expenses for its resolution, and the resolution duration which can last years. IDT has been the number one complaint to the FTC fifteen consecutive years (FTC 2015; ITRC 2014). Another indication of the rising tide and vulnerability is that more than 12.6 million adults in the U.S became victims of identity theft and lost a total of $21 billion to the thieves. Given the severity and vulnerability of the IDT occurrences, we expect that individuals intend to use CMI to control that danger. Response efficacy is the belief that the adaptive response will work, and that taking the protective action will be effective in averting the threat (Maddux and Rogers 1983). Self-efficacy is the belief that it is possible to implement the protective behavior. Together, both response efficacy and self-efficacy are termed perceived efficacy. When individuals believe that CMI will control the danger of IDT (i.e. high perceived response efficacy), and believe that they are capable of seeking and acquiring CMI (i.e. high self-efficacy), they will be willing to use CMI.

H1: Perceived severity positively influences intention to use CMI. H2: Perceived vulnerability positively influences intention to use CMI. H3: Response efficacy positively influences intention to use CMI. H4: Self-efficacy positively influences intention to use CMI

When individuals view losses from IDT as severe and perceive their vulnerability to experience IDT, we expect that this would generate fear. Fear is a negatively valenced emotion. We posit that if the severity and vulnerability of the threat of an identity theft is perceived, then fear will be an outcome of that perception. Therefore we hypothesize:

H5: Severity positively influences perceived fear. H6: Vulnerability positively influences perceived fear

Research on EPPM notes that fear affects intention when fear is high. That is, when fear is low, it does not have an effect on intention to self-protect, instead it has the opposite effect. It backfires. The boomerang effect of fear appeals is when fear decreases protection motivation instead of increasing it. Hence, low fear leads to maladaptive responses and not to adaptive responses. Results from prior research shows that there is no relationship between fear and adaptive response (intention) when there is low fear appeal manipulation (Boss et al. 2015). Based on the EPPM and the prior empirical results, we expect a direct effect of fear on intention to use CMI only when fear is high. Therefore, we hypothesize:

H7a: When high, fear has a direct effect on intention to use CMI. H7b: When low, fear has no direct effect on intention to use CMI

IDT represents a threat to the human asset, that is, the financial and psychological well-being of the individual (Kahn and Liñares-Zegarra 2015; Sharp et al. 2004). Johnston et al. (2015) argue the importance of including personal relevance factors in theories explaining protective behavior. Hence, we expect that an individual’s perception of their financial well-being (human asset) will affect their intention to use CMI. Therefore, we hypothesize:

H8: Perceived financial well-being positively influences intention to use CMI

FEAR CONTROL

EPPM suggests that perceived threat is the main contributing factor that determines how strong a response will be (intensity), whereas perceived efficacy is the main contributing factor that determines whether danger control or fear control processes is activated (Witte and Allen 2000). The notion is that when individuals doubt the efficacy of the recommended response, that is, when there are questions whether the recommended response will work (i.e. low perceived response efficacy) or when they doubt their ability to take the recommended action (i.e. low perceived self-efficacy), individuals will be motivated to control or reject their fear. This is usually done through denial or defensive avoidance (e.g. I am not at risk of identity theft, it cannot happen to me”). Therefore, we hypothesize:

H9: When threat is high and there is low response efficacy and low self-efficacy, there will be a higher degree of maladaptive responses (denial, avoidance) than when there is high response efficacy and high self-efficacy

METHODOLOGY

We will examine the proposed research model and hypotheses using an experiment. The EPPM suggests that the manipulation of the perceived efficacy denotes whether danger control or fear control process are enacted. Therefore, we intend to manipulate both perceived efficacy and threat by varying the levels of threat (severity and vulnerability) and efficacy (response efficacy and self-efficacy) in a 2 (high, low threat) x 2 (high, low efficacy) design. The responses of the participants will be measured immediately after the experiment. Our sample will include both students and non-students. All measures will be from the literature and adapted to the context of the current study. Severity, vulnerability, fear, self-efficacy, response efficacy and intent will be adopted from Boss et al. (2015) and Milne et al. (2002). Denial and avoidance will be adapted from Witte (1994). Financial well-being will be adapted from Prawitz et al. (2006).

EXPECTED RESULTS

We expect that perceived threat (severity and vulnerability) and perceived efficacy (self-efficacy and response efficacy) will be positively associated with intention to use CMI. In integrating EPPM with PMT, we also expect to show the importance of fear in understanding and predicting either the protective adaptive response represented with intention to use CMI or maladaptive defensive responses. This study seeks to highlight the need for IDT research in IS, and also add to literature.

REFERENCES

Albrecht, C., Albrecht, C., and Tzafrir, S. 2011. "How to Protect and Minimize Consumer Risk to Identity Theft," *Journal of Financial Crime* (18:4), pp. 405-414.

Anderson, K.B. 2005. "Identity Theft: Does the Risk Vary with Demographics?," *FTC, Bureau of Economics Working Paper*:279).

Boss, S.R., Galletta, D.F., Benjamin Lowry, P., Moody, G.D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors.," *MIS Quarterly* (39:4), 12//, pp. 837-864.

FTC. 2015. "Identity Theft Tops Ftc's Consumer Complaint Categories Again in 2014." Retrieved March 14, 2016, from https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014

Gonzales, A.R., and Majoras, D.P. 2007. "The President's Identity Theft Task Force: Combating Identity Theft a Strategic Plan."

Hemphill, T.A. 2001. "Identity Theft: A Cost of Business?," *Business and Society Review* (106:1), pp. 51-63.

ITRC. 2014. "Identity Theft Resource Center Breach Report Hits Record High in 2014." Retrieved September 4, 2015, from http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

Johnson, V.R. 2011. "Credit-Monitoring Damages in Cybersecurity Tort Litigation," *George Mason Law Review* (19:1).

Johnston, A.C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-A117.

Kahn, C.M., and Liñares-Zegarra, J.M. 2015. "Identity Theft and Consumer Payment Choice: Does Security Really Matter?," *Journal of Financial Services Research*), pp. 1-39.

Lai, F., Li, D., and Hsieh, C.-T. 2012. "Fighting Identity Theft: The Coping Perspective," *Decision Support Systems* (52:2), pp. 353-363.

Maddux, J.E., and Rogers, R.W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of experimental social psychology* (19:5), pp. 469-479.

Milne, G.R. 2003. "How Well Do Consumers Protect Themselves from Identity Theft?," *Journal of Consumer Affairs* (37:2), pp. 388-402.

Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British journal of health psychology* (7:2), pp. 163-184.

Prawitz, A.D., Garman, E.T., Sorhaindo, B., O'Neill, B., Kim, J., and Drentea, P. 2006. "Incharge Financial Distress/Financial Well-Being Scale: Development, Administration, and Score Interpretation," *Journal of Financial Counseling and Planning* (17:1).

Raghunathan, S., and Sarkar, S. 2016. "Competitive Bundling in Information Markets: A Seller-Side Analysis," *MIS Quarterly* (40:1), pp. 111-A145.

Roberts, L.D., Indermaur, D., and Spiranovic, C. 2013. "Fear of Cyber-Identity Theft and Related Fraudulent Activity," *Psychiatry, Psychology and Law* (20:3), pp. 315-328.

Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The journal of psychology* (91:1), pp. 93-114.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., and Hutton, S. 2004. "Exploring the Psychological and Somatic Impact of Identity Theft," *Journal of forensic sciences* (49:1), pp. 131-136.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communications Monographs* (59:4), pp. 329-349.

Witte, K. 1994. "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (Eppm)," *Communications Monographs* (61:2), pp. 113-134.

Witte, K. 1998. "Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Successes and Failures,").

Witte, K., and Allen, M. 2000. "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns," *Health education & behavior* (27:5), pp. 591-615.