Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2016 Proceedings

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

Winter 11-10-2016

A Picture vs. 1,000 Words: Threat Visualization and Verbalization in Information Security Fear Appeals

Vanessa Durner
University of Houston, vmdurner@bauer.uh.edu

Follow this and additional works at: http://aisel.aisnet.org/wisp2016

Recommended Citation
Durner, Vanessa, "A Picture vs. 1,000 Words: Threat Visualization and Verbalization in Information Security Fear Appeals" (2016). *WISP 2016 Proceedings*. 5.
http://aisel.aisnet.org/wisp2016/5

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2016 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Picture vs. 1,000 Words: Threat Visualization and Verbalization in Information Security Fear Appeals

Research in Progress

Vanessa Durner
University of Houston, Houston, Texas, USA {vmdurner@bauer.uh.edu}

ABSTRACT

Fear appeals are messages designed to persuade individuals to adopt a recommended behavior by describing the danger associated with a particular threat. This paper focuses on the persuasive roles of threat-related images and text in information security fear appeals and describes a series of studies that use neurophysiological measures to investigate how a fear appeal's threat verbalization and visualization drive emotion and cognition in order to motivate appropriate information security behavior.

Keywords: fear appeals, information security behavior, protection motivation, passwords

INTRODUCTION

Organizations currently face a substantial and expensive information security problem. In 2014, 42.8 million security breaches were reported, with the consolidated total cost of a single breach averaging $3.8 million (PricewaterhouseCoopers 2015). Organizations consequently need to motivate employees' information security behavior, which includes their conscious involvement in protecting information and information systems assets. Fear can lead individuals to take protective instructions more seriously (Witte 1992). The use of fear appeals is widespread and assumes that persuasion is enhanced when individuals are afraid (Dillard 1994). However, the impact of a fear appeal is not uniform across individuals, due to variations in perceptions of the appeal (Rogers 1983), and empirical research on the effectiveness of information security fear appeals has yielded mixed results (Johnston et al. 2015). Therefore, a better understanding

of the factors that influence perceptions of information security fear appeals would help organizations to craft fear appeals in ways that increases their persuasive effectiveness in motivating information security behavior.

Information security research on fear appeals tends to focus on threat verbalization via text-based fear appeal components, overlooking the motivating potential of threat visualization via image-based fear appeal components. By reproducing reality, image-based messages can elicit a variety of emotional responses (Messaris 1997). Consequently, images in fear appeals can evoke fear reactions, which can influence the process by which a fear appeal motivates behavior. To contribute to a better understanding of this process, this investigation focuses on the roles of fear appeal images and text in motivating information security behavior.

FEAR APPEAL COMPONENTS

Fear appeal theories such as the Extended Parallel Process Model (Witte 1992) and Protection Motivation Theory (Rogers 1983) argue that individuals evaluate a fear appeal's threat based on fear appeal components, leading to appraisals of the threat and recommended response that eventually can motivate the individuals to perform that response. Previous research has shown that information security fear appeals can promote various behavioral intentions and behaviors, such as individuals' intentions to install and run anti-spyware software (Johnston and Warkentin 2010), users' data backups (Boss et al. 2015), and decreased password reuse (Jenkins et al. 2014).

Fear appeals conventionally have four rhetorical components: threat severity, threat vulnerability, response efficacy, and self-efficacy (Rogers 1983; Witte 1992). However, other elements in a fear appeal have the potential to elicit fear and influence information security behavior. For example, a recent study suggests that the conventional fear appeal rhetorical framework is

inadequate for addressing information security threats, partially due to an absence of rhetoric that addresses threats of a personal nature (Johnston et al. 2015). Nevertheless, most research on information security fear appeals has focused on examining relationships among components of the fear appeal's message, perceptions of the message, and behavioral intentions (Johnston and Warkentin 2010). Thus far, this research has "only scratched the surface of the potential of fear as a motivator for security compliance" (Crossler et al. 2013, p. 93), even though both "in an information security context, both benevolent and malicious messages commonly attempt to elicit fear to motivate the target into action" (Anderson et al. 2016, p. 372).

Fear Appeals and Fear

Research in semiotics and marketing suggests that image-based messages elicit emotions due to the strong relationship between vision and emotion (Messaris 1997). Fear appeals with images can thus evoke stronger fear reactions than purely text-based messages, as demonstrated by research on warning messages on tobacco products (Hammond 2011; Ruiter et al. 2001). For example, a recent study has found that security warnings that include images with fear and disgust facial cues elicit higher recorded brain activity, reaction time, and self-reported attention compared to warnings without a facial image (Eargle et al. 2016), suggesting that individuals dedicate more attention and threat processing to security messages with threat-related images compared to security messages without images.

Even though prevalent fear appeal theories include fear arousal as a construct (Rogers 1983; Witte 1992), they fail to explain how a fear appeal can evoke fear and how fear in turn can motivate behavior (Dillard 1994). The following section outlines how threat visualization in fear appeals can elicit fear and focus attention on threat verbalization, which can subsequently provide evidence that motivates information security behavior.

CONCEPTUAL FRAMEWORK

Threat visualization is a fear appeal characteristic that represents the extent to which a fear appeal uses images to convey a specific danger that exists in a particular environment. A synthesis of the integrated process model for emotion (Elfenbein 2007) and a model of fear-processing circuitry from neuroscience (LeDoux 2000) suggests that exposure to a fear appeal initiates both immediate and delayed emotional registration, which represent the two neural pathways by which an individual becomes aware of and reacts to an emotional stimulus. These theoretical perspectives are appropriate for this investigation because they reflect the neural basis of emotion and the role of emotions as dynamic responses, as opposed to the tendency of many models to treat emotions as static and aggregate over time (Gooty et al. 2009).

Immediate emotional registration occurs when an individual processes sensory (e.g. visual) information associated with a fear appeal, and it influences how much attention is allocated to the fear appeal. In particular, as threat visualization increases, attention to the fear appeal should increase. This relationship is consistent with the results of a study that investigated attention to fear-relevant versus fear-irrelevant images (Öhman et al. 2001), which suggests that humans have a general bias to direct attention toward images with high threat visualization. Additionally, the semantic property of iconicity represents an image's ability to reproduce the appearance of reality and contributes to an image-based message's capability of evoking emotion (Messaris 1997). Because fear appeals with threat visualization inherently have greater iconicity than purely text-based fear appeals, they are more likely to elicit fear.

After a fear appeal image draws an individual's attention via immediate emotional registration, threat verbalization can influence delayed emotional registration and cognitive threat appraisal by conveying information related to threat severity (the negative implications for the individual associated with the threat) and threat vulnerability (the relevance of the threat to the individual). Threat verbalization thus includes a fear appeal's text-based evidence that is intended to convince an individual that a particular

threat is formidable and probable to some degree. Threat visualization can quickly draw attention to a fear appeal by concisely conveying danger, and it drives individuals to focus on threat verbalization, which provides evidence of the threat to convince them to adopt the recommended mitigation response.

METHODOLOGY

Neuro-information systems (NeuroIS) research applies cognitive neuroscience theories, methods, and tools to information systems research and focuses on biological metrics that indicate emotional state (vom Brocke and Liang 2014). NeuroIS is well-suited to this investigation because it facilitates measurement of the subconscious affective processes involved in emotional registration and emotional experience. Therefore, this approach will be adopted for a series of studies involving fear appeals that link passwords and identity theft. The studies described below use galvanic skin response (GSR) and facial expression analysis to investigate how fear appeals influence password behavior. Such measures are important because this investigation involves subconscious and potentially involuntary reactions.

The first study focuses on the individual influences of threat visualization and verbalization on fear, and will indicate the degree to which each threat component in a fear appeal individually elicits fear. For this study, 100 subjects have been recruited from a course that includes students from all undergraduate business majors. When subjects register for the study, they create a password-protected account (no restrictions on the password appear) and select a time slot to complete a survey and rate a series of images and sentences. The set of images includes computer-related images with varying levels of threat visualization, while the set of sentences includes sentences with varying levels of threat severity and threat vulnerability related to identity theft. The survey includes items related to perceptions of the threat and response (e.g. perceived threat severity). In the rating task, subjects indicate how each stimulus

makes them feel in terms of valence, arousal, and fear, while their facial expressions are recorded and evaluated using FaceReader software and their GSR is recorded to measure the physiological responses exhibited for each stimulus. These measurements will determine the relative levels of fear and emotion evoked separately by images and sentences associated with identity theft and passwords.

A second study focuses on the combined influence of threat visualization and verbalization on fear. As in the first study, subjects complete a rating task and survey while their facial expressions and GSR are recorded. The rating task stimuli include computer-related images with varying threat visualization combined with sentences with varying threat severity and threat vulnerability related to identity theft.

A final study addresses the influence of threat visualization and verbalization on fear and information security behavior. As in the first study, subjects create a password-protected account and sign up for the experimental task and survey. During the experimental task, subjects are randomly shown one of several fear appeals with varying threat severity, threat vulnerability, and threat visualization while subjects' facial expressions and GSR are recorded. Subject are then prompted to recreate their passwords.

CONCLUSION

This study will provide neurophysiological-based evidence about the degree to which elements of a fear appeal evoke fear and will establish the extent to which threat visualization and verbalization lead to improved information security behavior. This investigation will thus suggest ways to improve information security training and interventions by leveraging the fear appeal components that have the strongest influence on information security behavior.

REFERENCES

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., and Jenkins, J. L. 2016. "How Users Perceive and Respond to Security Messages: A NeuroIS Research Agenda and Empirical Study," *European Journal of Information Systems* (25:4), pp. 364-390.

Boss, S. R., Galletta, D. F., Lowry, P. B., 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), pp. 837-864.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90–101.

Dillard, J. P. 1994. "Rethinking the Study of Fear Appeals: An Emotional Perspective," *Communication Theory* (4:4), pp. 295-323.

Eargle, D., Galletta, D., Kirwan, B., Vance, A., and Jenkins, J. 2016. "Integrating Facial Cues of Threat into Security Warnings – an FMRI and Field Study," *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego.

Elfenbein, H. A. 2007. "Emotion in Organizations: A Review and Theoretical Integration.," *Academy of Management Annals* (1:1), p. 315.

Gooty, J., Gavin, M., and Ashkanasy, N. M. 2009. "Emotions Research in OB: The Challenges That Lie Ahead," *Journal of Organizational Behavior* (30:6), pp. 833-838.

Hammond, D. 2011. "Health Warning Messages on Tobacco Products: A Review," *Tobacco Control* (20), pp. 327-337.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., and Lowry, P. B. 2014. "Improving Password Cybersecurity through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals," *Information Technology for Development* (20:2), pp. 196-213.

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

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.

LeDoux, J. E. 2000. "Emotion Circuits in the Brain," *Annual Review Of Neuroscience* (23), pp. 155-184.

Messaris, P. 1997. *Visual Persuasion: The Role of Images in Advertising*. SAGE Publications.

Öhman, A., Flykt, A., and Esteves, F. 2001. "Emotion Drives Attention: Detecting the Snake in the Grass," *Journal of Experimental Psychology* (130:3), pp. 466-478.

PricewaterhouseCoopers. 2015. "The Global State of Information Security Survey 2015" from http://www.pwccn.com/home/eng/rcs_info_security_2015.html.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," *Social Psychophysiology*, pp. 153-176.

Ruiter, R. A. C., Abraham, C., and Kok, G. 2001. "Scary Warnings and Rational Precautions: A Review of the Psychology of Fear Appeals.," *Psychology & Health* (16:6), pp. 613-631.

vom Brocke, J., and Liang, T.-P. 2014. "Guidelines for Neuroscience Studies in Information Systems Research," *Journal of Management Information Systems* (30:4), pp. 211-234.

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