Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings | Midwest (MWAIS)

5-2018

The Role of Message Structure on the Effectiveness of Security Messages: A Neuro-Investigation

Roozmehr Safi
University of Missouri–Kansas City, safir@umkc.edu

Glenn J. Browne
Texas Tech University, glenn.browne@ttu.edu

Eric Walden
Texas Tech University, eric.walden@ttu.edu

Follow this and additional works at: http://aisel.aisnet.org/mwais2018

Recommended Citation
Safi, Roozmehr; Browne, Glenn J.; and Walden, Eric, "The Role of Message Structure on the Effectiveness of Security Messages: A Neuro-Investigation" (2018). *MWAIS 2018 Proceedings*. 34.
http://aisel.aisnet.org/mwais2018/34

This material is brought to you by the Midwest (MWAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MWAIS 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Role of Message Structure on the Effectiveness of Security Messages: A Neuro-Investigation

(Research-in-progress)

Roozmehr Safi
University of Missouri–Kansas City
safir@umkc.edu

Glenn J. Browne
Texas Tech University
glenn.browne@ttu.edu

Eric Walden
Texas Tech University
eric.walden@ttu.edu

ABSTRACT

Identifying effective methods for persuading computer users to adhere to information security guidelines is a major preoccupation of security researchers and practitioners. In this study we investigate how different message structures can affect the persuasive power of information security communications. We use a 2 X 2 factorial design to investigate the role of message framing (either positive or negative) and message advocacy (prevention-oriented or detection-oriented) on listeners. In this research, in addition to collecting behavioral results (i.e., self-reports), we collect brain data using the fMRI technique, which allows us to form a more complete understanding of the cognitive processes underlying message comprehension. In this document, we discuss the research questions, the experimental procedures, as well as the anticipated implications of this research-in-progress for information security theory and practice.

Keywords

Information security, message framing, preventing security incidents, detecting security incidents, fMRI.

INTRODUCTION

Statistics show a sharp increase in the number of computer security-related incidents. These statistics attribute many of such incidents to individual users' (mis)behaviors. Security researchers have employed various approaches to enhance computer users' security behavior. Of all these approaches, training is the most commonly used method (Puhakainen and Siponen 2010). Nevertheless, the training methods currently used have time and time again proved to be far from effective. According to the literature of social psychology, the relationship between knowledge, attitude, and behavior is far from deterministic (Petty and Krosnick 2014) (p. 382). Enhancing users' behavior toward security, therefore, may require persuasive initiatives other than increasing users' knowledge alone. One such method is finding certain features or attributes for security messages that contribute to their persuasive power. The aim of the current research-in-progress is to partly fill this gap in the domain of IS.

THEORY

To resolve the apparent confusion in the field of framing effects research, Levin, Schneider, and Gaeth (1998) developed a typology to distinguish between three different types of valence framing effects: risky choice framing, attribute framing, and goal framing. Previous empirical studies conducted mainly in the domains of health and public management have documented that goal framing can be used as an effective method to enhance the persuasive power of messages. Goal framing can be described as follows: to persuade subjects to adopt a certain behavior, a communicator can state, or "frame," facts and information differently. For example, the communicator can either highlight the positive consequences of engaging in the behavior (i.e., positive, or gain framing), or highlight the negative consequences of not engaging in the behavior (i.e., negative, or loss framing). Some researchers have reported that certain types of frames are more effective for promoting certain types of tasks: that prevention-oriented messages are more persuasive if positively framed and that detection oriented messages are more effective if negatively framed (Salovey et al. 2002). We test this hypothesis in the context of information systems, since similar to the domain of health, prevention and detection are two major methods for mitigating security risks in IS.

PROCEDURES AND FUTURE STEPS

To investigate the effects of advocacy, framing, and their interaction on persuasiveness of security messages we created 45 messages promoting the use of antimalware software. Antimalware software is useful for both preventing and detecting threats, and therefore is a good choice of security product for the purpose of this study. Four different variations of each of the 45 messages were created for presenting to subjects: Prevention-Positive (P+), Prevention-Negative (P-), Detection-Positive (D+), and Detection Negative (D-). As an example, the P+ version of one of the messages reads "If you do install an anti-malware program, you will be preventing loss of memorable pictures.", while the D- version of the message reads: "If you don't install an anti-malware program, you won't be detecting loss of memorable pictures." The 180 statements were presented in random order to each of the subjects. Each of these statements was shown for a period of five seconds. After each statement, participants' self-reported evaluations of the persuasiveness of the message was elicited (a binary, yes/no answer). The procedure was conducted in an fMRI scanner, so brain activity was captured as subjects processed and evaluated the messages. In the next step, the behavioral results as well as the brain data will be analyzed.

CONCLUSION

In this research-in-progress, we investigate the role of message structure on the persuasive power of security communications. Supplementing behavioral results with brain data in this study is particularly beneficial from a number of perspectives. First, the use of neuro-techniques allows for capturing unconscious or hidden cognitive processing involved in performing the task (in this case, processing security messages). Second, it can provide a more direct "reading" of the brain by capturing objective answers that are presumably free of conventional measurement inaccuracies or response biases (e.g., social desirability bias) (Dimoka et al. 2011). We expect the theoretical and the practical implications of findings from this research to go beyond the field of IS to inform other fields involving communicating risk-related messages, such as health and general safety and security.

REFERENCES

1. Dimoka, A., Pavlou, P. A., and Davis, F. D. 2011, Research Commentary—Neurois: The Potential of Cognitive Neuroscience for Information Systems Research, *Information Systems Research*, 22, 4, 687-702.
2. Levin, I. P., Schneider, S. L., and Gaeth, G. J. 1998, All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects, *Organizational Behavior and Human Decision Processes*, 76, 2, 149-188.
3. Petty, R. E., and Krosnick, J. A. 2014. Attitude Strength: Antecedents and Consequences. Psychology Press.
4. Puhakainen, P., and Siponen, M. 2010, Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, *MIS Quarterly*, 34, 4, 757-778.
5. Salovey, P., Schneider, T. R., and Apanovitch, A. M. 2002., Message Framing in the Prevention and Early Detection of Illness, The Persuasion Handbook: Developments in Theory and Practice, pp. 391-406.