Winter 12-13-2018

FEAR APPEALS VERSUS PRIMING IN RANSOMWARE TRAINING

Michael Curry
michael.curry@wsu.edu

Byron Marshall
byron.marshall@bus.oregonstate.edu

Robert E. Crossler
rob.crossler@wsu.edu

John Correia
john.correia@wsu.edu

FEAR APPEALS VERSUS PRIMING IN RANSOMWARE TRAINING

Curry, Michael[a.,c.], Marshall, Byron[b], Crossler, Robert .E.[a],. Correia, John [a.]

[a.] *Carson College of Businesses, Washington State University*

[b.] *College of Business, Oregon State University*

[c.] *Corresponding Author*

Abstract

Employee non-compliance is at the heart of many of today's security incidents. Training programs often employ fear appeals to motivate individuals to follow policy and take action to reduce security risks. While the literature shows that fear appeals drive intent to comply, there is much less evidence of their impact after intention is formed. Building on IPAM – a process nuanced model for compliance training and assessment – this study contrasts the impact of fear appeals vs. self-efficacy priming on ransomware training. In our proposed study, a pool of students will participate in a three-step series of training events. Some participants will encounter enhanced fear appeals at each step while others will be presented with materials that include priming signals intended to foster development of increased self-efficacy. Previously identified drivers of behavior (intent, processed-nuanced forms of self-efficacy, and outcome expectations) are measured so that the effect of the treatments can be contrasted. A scenario agreement methodology is used to indicate behavior as a dependent variable. We expect to show that while fear appeals are useful and help build intent to comply at the motivational stage, process-nuanced self-efficacy treatments are expected have a stronger effect on behavior post-intentional.

Keywords: Security, behavior change, ransomware, fear appeals, self-efficacy, content priming.

Introduction

Employee non-compliance with security guidance is widely regarded as one of the weakest links in cybersecurity (Verizon Enterprise Solutions 2018), exposing organizations to significant risks. For example, ransomware's primary threat vectors exploit human as well as technical weaknesses, (FBI 2017; Verizon Enterprise Solutions 2018) suggesting that responsible behavior is a pressing issue in cyber security. Ransomware is considered the most significant malware problem facing individuals and organizations today (O'Brien 2017; Verizon Enterprise Solutions 2018). The speed at which ransomware became a global threat illustrates the common problem for cybersecurity professionals who must update their recommended best practices, and for employees who must be trained on those new practices.

According to the InfoSec Process Action Model (IPAM) (Curry et al. 2018), a recently proposed process-nuanced theory of behavior, effective training involves identifying stages of behavior change, then targeting individuals with treatments that promote transition from one stage to the next. IPAM effective training is a process in which people gain knowledge and become motivated and mindful about implementing compliance behaviors. This model incorporates new constructs to security research for assessing the transition from post-intentional to plans for initiating action and full recovery from an old behavior.

Fear appeals are a prominent approach used in information security (InfoSec) research to influence security behavior changes and scare individuals to adopt a security behavior. Fear appeals have demonstrated increased compliance with recommended measures (e.g., Boss et al. 2015; Johnston et al. 2015). However, a noticeable gap in the InfoSec research exists where the majority of fear appeals research is focused on the intention towards security policy compliance. The IPAM theory posits that post-intentional, risk awareness messages may be less effective than those which promote turning good intentions into action through different formulations of self-efficacy.

In this study we propose to contrast the use of fear appeals with self-efficacy boosting using content priming for promoting multiple protective-motivation behaviors (PMBs). Priming is an implicit approach to frame the thinking of individuals as they participate in interactions with survey materials to influence subsequent behavior. Our research questions focus on the relative impact of priming in training. Are well-designed but relatively small priming features sufficient to impact perceived self-efficacy? Can content priming facilitate development of process nuanced self-efficacy perceptions in an InfoSec training context? Can differences in the effect of priming versus fear appeals be explain by the PMB categorizations? Do these self-efficacy influencers have as much of a positive effect on behavior as multiple instances of fear appeals? If priming is more effective than fear appeals in influencing compliance post-intentional, then organizations will be able to use these insights to build improved training programs and better mitigate security risks.

Contributions, Limitations and Conclusions

This study's contribution is offering compelling evidence that while fear appeals are effective as a motivation of intention formation they may not be as effective post intentions. It also offers additional support for the IPAM phased approach to security research by demonstrating the value of volitional phase drivers of behavior. A limitation of the study is the assumption that training is a useful proxy for ransomware preparedness, while a more robust experimental design might evaluate actual ability to avoid and recover from ransomware. In conclusion, this study has great potential to advance our theoretical understanding of security behavior change with practical implications for both researchers and managers.

REFERENCES

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 Behaviours,” *MIS Quarterly* (39:4), pp. 837–864. (https://doi.org/10.25300/MISQ/2015/39.4.5).

Curry, M., Marshall, B., Crossler, R. E., and Correia, J. 2018. “InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior,” *Data Base for Advances in Information Systems* (49:S1), pp. 49–66. (https://doi.org/10.1145/3210530.3210535).

FBI. 2017. “2017 Internet Crime Report.” (https://pdf.ic3.gov/2017_IC3Report.pdf).

Johnston, A., 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. 113–134.

O’Brien, D. (Symantec). 2017. “Internet Security Report Ransomware 2107.” (https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf).

Schwarzer, R., and Luszczynska, A. 2008. “How to Overcome Health-Compromising Behaviors: The Health Action Process Approach,” *European Psychologist*. (http://econtent.hogrefe.com/doi/abs/10.1027/1016-9040.13.2.141).

Verizon Enterprise Solutions. 2018. “2018 Data Breach Investigations Report.” (http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf).