

Winter 12-10-2016

# What's it worth to you? Applying risk tradeoff paradigms to explain user interactions with interruptive security messages

David Eargle

*University of Pittsburgh*, [dave@daveeargle.com](mailto:dave@daveeargle.com)

Dennis F. Galletta

*University of Pittsburgh - Main Campus*, [galletta@katz.pitt.edu](mailto:galletta@katz.pitt.edu)

Jeffrey L. Jenkins

*University of Arizona*, [jeffrey\\_jenkins@byu.edu](mailto:jeffrey_jenkins@byu.edu)

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

---

## Recommended Citation

Eargle, David; Galletta, Dennis F.; and Jenkins, Jeffrey L., "What's it worth to you? Applying risk tradeoff paradigms to explain user interactions with interruptive security messages" (2016). *WISP 2016 Proceedings*. 14.

<http://aisel.aisnet.org/wisp2016/14>

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](mailto:elibrary@aisnet.org).

## **What's it worth to you? Applying risk tradeoff paradigms to explain user interactions with interruptive security messages**

**David Eargle**

Katz Graduate School of Business, University of Pittsburgh, USA  
[dave@daveeargle.com](mailto:dave@daveeargle.com)

**Dennis Galletta**

Katz Graduate School of Business, University of Pittsburgh, USA  
[galletta@katz.pitt.edu](mailto:galletta@katz.pitt.edu)

**Jeff Jenkins**

Information Systems Department, Brigham Young University, USA  
[jeffrey\\_jenkins@byu.edu](mailto:jeffrey_jenkins@byu.edu)

### **ABSTRACT**

Attacks on information security continue to result in large losses for organizations. Oftentimes, the breaches occur because organizational insiders fail to adhere to commonplace system security messages. This could be because, faced with the challenges and time demands of everyday stressors, security policy compliance can be costly for individuals; security actions require time and distract attention from other primary tasks. To defend against these attacks, user interactions with security messages need to be better understood.

This study reports the results of a 110-participant MTurk field study that examines user interactions with interruptive security messages through the lens of a risk tradeoff paradigm. First, a gap in the information security literature is identified, wherein findings about low security-message attention are contrasted against studies that assume attention and information processing. Three competing hypotheses are proposed that describe different patterns of risk analysis that users may engage in when interacting with an interruptive security message: (1) very little to no elaboration over the risk-taking decision due to perniciously low attention, (2) consistent security message risk-taking decision elaboration, and (3) a bimodal situation where elaboration depends on the information security risk-reward tradeoff balance. Multiple

behavioral dependent variables are corroborated to support the third hypothesis, suggesting the existence of a bimodal risk tradeoff paradigm for user interactions with interruptive security messages. The relevance of the findings for research and practice are discussed.

**Keywords:** interruptive security messages, risk tradeoff, heuristic-systematic model, attention

## INTRODUCTION

Abundant stories in media reports about organizations falling victim to security hacks describe huge financial and operational damage from those attacks. While the victims would often have the public believe that these hacks are the result of “highly sophisticated” attack vectors (Gallagher 2016), the reality is that the breaches often grow from simple inlets, including users who fail to observe basic security policies such as using caution when opening unsolicited email attachments. Even simple social engineering attack vectors such as these can have disastrous, potentially life-threatening consequences. For example, security researchers have observed devastating ransomware being delivered via phishing attacks and infected software and documents (Goodin 2016). These attacks count on users to ignore commonplace security messages, such as the Microsoft Office macro warning (Goodin 2016; Schneier 2011).

Information security research has explored why individuals violate security policies and fall victim to attacks. Some studies make an underlying assumption that users make active risk-taking assessments for every security decision, prompted by security messages (Boss et al. 2015; Johnston et al. 2015). A “lazy user” perspective depicts security as an unnecessary burden that should be bypassed if possible. Many studies use deterrence theory, testing the efficacy of using sanctions to influence security-related decision making (e.g., D’Arcy and Herath 2011; Johnston et al. 2015). Another camp takes the position that “users are not the enemy” (Adams and Sasse 1999), eschewing criminology-inspired sanctioning deterrence, and attributing security

misbehavior largely to inattention and habituation (e.g., Anderson et al. 2016a; Anderson et al. 2016c). In this view, if a security message is ignored, the design of the interface is to blame. We question how these two stances coexist – purposeful risk-taking security decision making does not seem congruous with inattentive dismissal of security messages.

The purpose of this study is to attempt to reconcile the differences between the two camps of research on user interactions with security messages. In our study, we employ a between-subjects repeated-measures field study using Amazon Mechanical Turk with 110 subjects. In our design, we influence the risk-taking tradeoff by varying the value of adhering to security messages. Corroborating several dependent variables, including security choice, reaction times, and mouse-cursor movements measures, we discover an interesting bimodal pattern where elevated attention and risk-taking elaboration are present only until the risk tradeoff passes a certain threshold.

## **LITERATURE REVIEW, THEORY AND HYPOTHESES**

### **SECURITY MESSAGE INATTENTION**

A major contributor to security message failure is a simple lack of attention (see Anderson et al. 2016b). Inattention to security messages has been attributed to a neurobiological process wherein users reach a state of habituation after repeated exposure: when presented with a security message, a user draws on memory to inform a response instead of actively reviewing and elaborating the current message. While habituation has been blamed in several studies for observed security message disregard (Bravo-Lillo et al. 2014; Bravo-Lillo et al. 2013), NeuroIS tools including fMRI (Anderson et al. 2016c) and eye tracking (Anderson et al. 2016a) have directly measured habituation processes and reliance on memory. Changing the appearance of the warning message has been effective in combatting habituation (Anderson et al. 2016c).

Alarming, some of the studies have found no differences in user reactions to security messages even when the severity of the communicated threat is increased (e.g., Bravo-Lillo et al. 2014; Schechter et al. 2007). However, these studies do not claim that users perceive higher levels of threat despite the message having changed. Indeed, often in these studies, nuanced changes are not perceived at all due to habituation's recall rather than active processing of changed stimuli.

Drawing on these attention findings, one possible pattern is that users rarely engage in risk-taking assessments when interacting with security messages, regardless of varying levels of tradeoff in the risk-taking decision. This would suggest that users are habituated to the messages, and are performing automatic, learned responses when encountering new ones. If this is true, then research should focus mainly on fostering attention to the messages, so as to increase the likelihood that users will engage with the messages and make meaningful choices.

*H1: There will be no difference in markers of cognition between varying risk-taking tradeoff levels (i.e., there will be no evidence of risk-taking assessments).*

## **RISK TRADEOFFS**

Risk has been studied in an information security context typically through the lens of protection motivation theory (Rogers 1983), wherein the constructs of threat severity and threat susceptibility essentially represent the security threat's risk levels (Boss et al. 2015; Johnston et al. 2015; Johnston and Warkentin 2010). Individual differences in risk perceptions have also been used to predict security message disregard (Vance et al. 2014).

In this study, we consider a different facet of information security risk -- the risk tradeoff associated with *adhering* to the security message. Inherent in the idea of risk is that there is something to be gained from taking the risk. In the finance literature, risk tradeoff is quantifiable as the potential return on investment, with willingness to accept the risk being a function of the

magnitude of the return (Ghysels et al. 2005). This same concept of risk-taking behavior being positively associated with the potential gains or loss-avoidance involved has also been described in the behavioral economics literature (e.g., Kahneman and Tversky 1979).

Risk-tradeoff applies to the context of information security messages in that one risks a security threat in exchange for some benefit. Guo et al. (2011) captures the motivation to intentionally violate organizational information security policies with their "relative advantage for job performance [from violating a policy]" measure. Interruptive security messages often block or hinder users from completing their primary tasks (Jenkins et al. 2016). Observance of the security policy adds stress and requires more effort to complete the primary task. Failing to complete the task or taking longer to complete it may lead to poor employee performance evaluations (Lowry and Moody 2015). To capture these tradeoffs, we will vary the "penalties" associated with *heeding* the message, while holding constant security threat severity and susceptibility.

We use the risk-taking paradigm to propose an alternative to H1, wherein users nearly *always* engage in risk-taking assessments when encountering security messages, with the degree of security decision elaboration depending on the tradeoff weights. This view assumes that attention is sufficiently present to prompt risk-tradeoff appraisals, and supports studying the impact of levels of perceived risk on users' security message risk-taking assessments. Those tradeoff assessments can be discerned if greater evidence of elaboration and cognition is present as the tradeoff scale is increasingly tipped.

*H2: The pattern of risk-taking will be linear: the markers of cognition will linearly increase, dependent on the level of risk-taking tradeoff.*

## COGNITIVE ELABORATION AS A FUNCTION OF RISK-TRADEOFF BALANCE

The third hypothesis combines aspects of the first two, drawing from principles of the heuristic-systematic model of information processing (HSM) (Chen and Chaiken 1999) to predict whether a user will cognitively engage with a security warning. HSM, a theory of persuasion, finds early expression in the script concept (Abelson 1981). The script concept asserts that an individual will follow a “script” and grant small requests without cognitive elaboration, as long as a reason is given. Individuals will be likely to perform this script unless (1) the script is broken by not providing a reason or if (2) the request is large, in which case they will elaborate over the request and the reason before deciding whether to accept it.

We predict that the perceived risks involved will impact whether or not a user elaborates over a security-message decision. To our knowledge, while HSM has been evaluated in a risk judgement paradigm (Trumbo 2002), the impact of the balance of the risk tradeoff has not been examined in an HSM frame. We will manipulate the risks involved for *heeding* the warning. If the script theory concept or HSM elaboration prediction holds, we expect to see a bimodal distribution of behavior across risk levels, where after a certain threshold of risk tradeoff for *adhering* to the message is surpassed, elaboration will be much less likely. From the habituation-theory lens, the scripted behavior would rely on memory and pay little attention to the security message (c.f. Böhme and Köpsell 2010; Sunshine et al. 2009). The tradeoff behavior will involve whatever task was interrupted by the security message. If adhering to the message will not adversely impact the interrupted task, elaboration over the decision should be more likely to occur. In summary, we posit that if users perceive that the benefits of heeding a warning are close to the accompanying losses (e.g., time lost or inability to complete an objective), then they will more carefully consider the risk tradeoff before making a decision. However, if the tradeoff

choice is clear, then users will be less likely to engage in elaboration, and instead their behavior will more closely follow patterns of lower attention and automatic choices.

*H3: The pattern of risk-taking will be modal. The risk decision will be elaborated over, as long as a threshold of risk-benefit balance has not been exceeded.*

We note that our hypotheses are mutually exclusive. They each describe different patterns of attention and risk-taking assessments that users may follow.

## **METHODOLOGY**

We used a field study with a between-subjects repeated-measures design. We recruited 110 participants from the United States using Amazon's Mechanical Turk platform. Participants were directed to a server under our control running our experiment codebase, built on the psiTurk framework (McDonnell et al. 2012), where they were randomly assigned to one of three treatment groups. Data from Mechanical Turk has been found to be as reliable as data from other U.S. survey panels (Steelman et al. 2014), and more importantly, they are likely to be using their own computers, raising their sense of perceived risk (c.f. Boss et al. 2015; Vance et al. 2014).

We used an IRB-approved deception protocol. The pretense was that participants were performing an image classification task, when in reality, we were interested in users' behaviors when they were presented with interruptive security messages. The image classification ruse and the security warning presentation are described below.


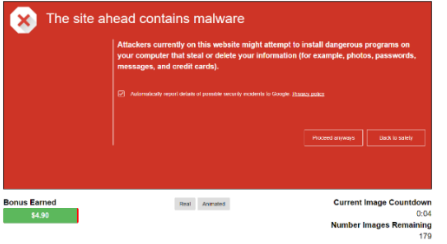
Participants performed a modified version of the image classification task described in Vance et al. (2014). In our task, participants were told that they would classify a series of images in order to help test a computer classification algorithm. It was explained that a series of live, external websites would be loaded into a frame in the center of the webpage (i.e., an `iframe` HTML element). For each page load, participants were asked to classify whether the image was a photograph of Batman or an artist's rendering. On top of a \$1.00 base payment, participants



were offered an additional \$1.00 performance-based bonus payment. Each incorrect classification results in a “penalty” decrease in their bonus payment, with the penalty amount depending on a participant’s treatment group. Three penalty level treatment groups were used: 5, 10, and 25 cents. We chose these increments because they mapped naturally to U.S. coinage. Furthermore, to encourage attention to the task, we warned that too many incorrect responses would result in their work being rejected with forfeiture of any payment. Participants’ current bonus status was depicted with an animated and labeled bar beneath the central `iframe`. Participants were encouraged to move quickly, limiting them to a maximum of 10 seconds for each classification. A timeout resulted in the classification being marked as “incorrect.” After a 4-image practice round, participants classified 75 images. See Figure 1 for an example screenshot of the image classification protocol.

Five times during the task, the page load within the central window was interrupted with a browser security warning. The warning, based on Google Chrome malware warning build 51.0.2704.63 m, signaled that continuing to load the page would result in the visitor’s computer becoming infected with malicious software (“malware”). The warning had a button allowing the user to proceed past the warning to the website (see Figure 2).

If, while a security warning was shown, participants made a guess about whether the image on the unseen screen was real or animated, they risked being marked wrong. Because each incorrect classification decreased the bonus earned and increased the likelihood of a participant’s work being rejected, participants were financially motivated to ignore the warning.

	
<p>Figure 1 – Example of image classification task demonstrating loaded page window and task control panel (adapted from Vance et al. 2014).</p>	<p>Figure 2 – The security warning as it appeared to participants. Based on the Google Chrome malware warning, from build version 51.0.2704.63 m</p>

## METRICS

We consider various markers of security behaviors and cognition. First, we test for differences in actual security message adherence (choosing to load the site despite the warning) among treatment groups. Second, we test for differences in reaction time among treatment groups. Reaction time, a form of mental chronology, is a commonly-used metric for cognitive effort (Jensen 2006). Third, we test for differences in cognitive engagement by examining *area under the curve* (AUC), a mouse-cursor movement statistic (Hibbeln et al. 2016; Jenkins et al. 2016). For AUC, the more the line connecting the mouse cursor starting and ending point for a security warning impression deviated from a straight-line trajectory, the greater the evidence of higher levels of cognitive processing.

## RESULTS

### WARNING ADHERENCE RATES

To test for differences in adherence rates (whether a participant ignored a warning), we performed an empirical logit analysis (Barr 2008). We specified a fixed effect for treatment group, a fixed effect for the number of warnings seen, and a random intercept for each participant. An ANOVA found significant differences among treatment groups on whether the warning was ignored,  $Wald \chi^2(2) = 11.502, p = .003$ . Averaged across warning exposures, participants in the 5-cent penalty treatment group were 32% less likely to ignore the warning

than were participants in the 10-cent penalty treatment group ( $p = .001$ ), and 39% less likely to ignore the warning than participants in the 25-cent penalty treatment group ( $p < .001$ ).

However, there were no significant differences among log odds comparing the 10-cent group to the 25-cent group. Furthermore, while there was an overall 5% increase in the odds of ignoring the warning for each additional warning exposure ( $p = .021$ ), there was no interaction between treatment group and number of warnings seen ( $Wald \chi^2(2) = .875, p = .646$ ). Model parameters are graphically displayed in Figure 3.

### **REACTION TIME**

We tested for the impact of treatment group on a log transformation of reaction time using a linear mixed model with random intercept for each participant, along with fixed effects for treatment condition, number of warnings seen, plus an interaction between the fixed effects. Significant differences were found on time taken among the treatment groups,  $Wald \chi^2(2) = 7.684, p = .022$ . Averaging across warning exposures, participants in the 5-cent treatment group had 22.7% slower reaction times than did participants in the 10-cent treatment group ( $p = .008$ ), and 15.1% slower reaction times than participants in the 25-cent treatment group, ( $p = .075$ ). There were no significant differences between reaction times averaged across warning exposures for participants in the 10-cent group compared to the 25-cent treatment group ( $p = .430$ ). Also, the interaction effect of penalty treatment and number of warnings seen was not statistically significant,  $Wald \chi^2(2) = 1.642, p = .440$ . See Figure 4.

### **MOUSE-CURSOR MOVEMENT**

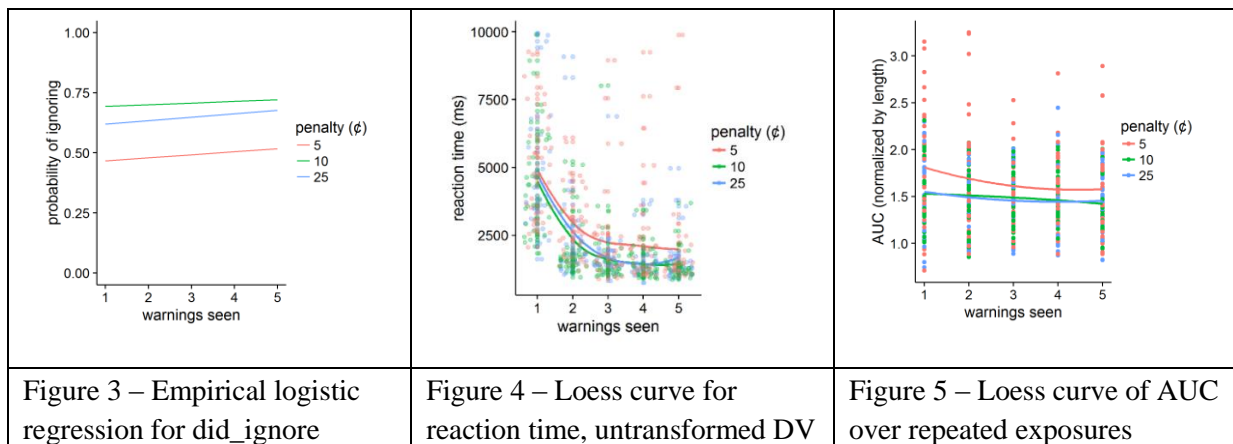
We performed analyses on the log-transformation of the length-normalized AUC. For our first analysis of this dependent variable, we only considered the first warning exposure for each participant. Significant differences were found among the treatment groups on AUC,  $F(2,95) =$

3.198,  $p = .045$ . Post-hoc analyses indicated that participants in the 5-cent treatment group had marginally higher AUC than did participants in either the 10-cent treatment group or the 25-cent treatment group ( $p = .055$  and  $p = .022$  respectively). No significant differences were found in AUC between participants in the 10- and 25-cent treatment groups ( $p = .681$ ).

Next, we added a fixed effect to the model, counting each warning seen for each participant, a fixed effect for the interaction between treatment group and number of warnings seen, plus a random intercept for each participant. Unlike the first analysis, this analysis only found the main effect of number of warnings seen to be significant ( $\chi^2(1) = 16.559, p < .001$ ). Neither the interaction effect nor the main effect of treatment group were found to be significant ( $p = .295$  and  $p = .205$  respectively). See the Loess curve in Figure 5.

### DISCUSSION

We tested for differences on various outcomes: (1) actual adherence rates, (2) reaction times, and (3) mouse cursor movement AUC. For the actual adherence rates, participants who were only penalized 5 cents per incorrect answer were much less likely to ignore the warning than participants who were penalized either 10-cents or 25-cents per incorrect response. This was expected – a penalty of 10 cents and 25 cents represented losses of 10% and 25% of the available \$1.00 bonus that participants stood to earn, respectively. Using a risk tradeoff paradigm,



participants appeared to be more likely to trade 5% of their bonus to avoid a security risk than they were to trade either 10% or 25%. One interesting observation is that there were no observed differences in adherence rates between the 10-cent and 25-cent treatment groups. This suggests that the risk-analysis tradeoff that individuals engage in is not linear, but rather, that it is modal, supporting H3. In this study, a 10% penalty – a mere 5% increase over the lower treatment group – was sufficient to boost substantially the rates of ignoring security warning–by 20%. Individuals at work may engage in these risk-taking tradeoffs when they are interrupted by security messages. Time lost through adhering to the security warning and finding a workaround may result in negative outcomes such as missing a work deadline. Depending on the weight of these negative outcomes compared to the perceived benefits of avoiding the security threat, similar warning adherence patterns as seen in our study may be observed in the workplace.

By comparing these results to our other outcome measures indicative of attention and cognitive processing across treatment groups, we gain insights into the level of cognition and attention that participants exhibited. Participants in the 5-cent treatment group had the longest reaction times to the warnings, even across multiple exposures. All else equal, longer reaction times in decision-making are suggestive of greater levels of attention and cognition (Jensen 2006). Therefore, the faster reaction times in the 10-cent and 25-cent penalty groups suggest that participants viewed their choice as being more straightforward. The same pattern of results between treatment groups was seen in the analysis of mouse-cursor movement AUC for first warning impressions. We know from the analysis of the adherence data that participants were more likely to ignore the warning in these higher penalty groups. We can therefore begin to make the case that automatic, mindless reactions to security messages are more likely after a risk tradeoff threshold is surpassed. But, participants apparently do *not* indiscriminately ignore all

warnings. Participants in the 5-cent treatment group appeared to be more likely to engage in risk-benefit tradeoff decision-making and to elaborate over the security decisions. In short, participants do not *always* respond mindlessly to security messages, rejecting H1. But these results suggest that they *often* do, rejecting H2.

It is worth noting that when differences were tested for AUC averaged across time, no differences were found. Only the differences in group intercepts (the first warning impressions) were statistically significant. This may be explained by participants only engaging in the risk-taking elaboration *once*. Future security warning decisions may have been similar enough to the first that re-elaboration was not necessary. This observation of a decrease in elaboration over repeated exposures is in line with the principle of habituation to security messages (c.f. Anderson et al. 2016a; Anderson et al. 2016b; Anderson et al. 2016c).

A greater number of treatment groups would be necessary to determine the number of modes for interruptive security warning risk-taking decisions. For situations where the tradeoff quantification is less immediately quantifiable than our money-penalty operationalization, a model would be useful to describe what perceptual factors best predict the tradeoff values that participants use when they engage in evaluation of the security message risk-taking tradeoff. Such a model could build on the information security policy violation intention models already in existence (e.g., D'Arcy and Herath 2011). Organizations can modify their incentive structures to *decrease* the tradeoff amount that organizational insiders discern when considering whether to adhere to a warning, perhaps through threat of sanctions for non-security-message adherence (D'Arcy and Herath 2011; Johnston et al. 2015), or through rewards for good security hygiene. Security message design can also aim to boost perceptions of threat severity and susceptibility, which may also tip the risk-tradeoff decision further.

## CONCLUSION

This study has investigated a gap in information security literature between assumptions of high and low user attention to interruptive security messages. Using an interruptive security message context, the corroboration of multiple dependent variables from a field study supported the existence of users behaving under a bimodal risk tradeoff paradigm, where security message elaboration was dependent on the risk tradeoff balance between the perceived information threat and the losses involved in not being able to perform the interrupted task. Future research should be performed to further investigate users' risk perceptions when interacting with interruptive security messages, including how to manipulate these perceptions. This line of inquiry holds great promise for both research and practice.

## REFERENCES

- Abelson, R. P. 1981. "Psychological Status of the Script Concept," *American Psychologist*, (36:7), pp. 715-729.
- Adams, A., and Sasse, M. A. 1999. "Users Are Not the Enemy," *Communications of the ACM*, (42:12), pp. 40-46.
- Anderson, B. B., Jenkins, J., Vance, A., Kirwan, C. B., and Eargle, D. 2016a. "Your Memory Is Working against You: How Eye Tracking and Memory Explain Habituation to Security Warnings," *Decision Support Systems*, (Forthcoming).
- Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., and Jenkins, J. L. 2016b. "How Users Perceive and Respond to Security Messages: A NeuroIS Research Agenda and Empirical Study," *European Journal of Information Systems*, (Advance online publication).
- Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J., and Eargle, D. 2016c. "From Warnings to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It," *Journal of Management Information Systems*, (Forthcoming).
- Barr, D. J. 2008. "Analyzing 'Visual World' Eyetracking Data Using Multilevel Logistic Regression," *Journal of Memory and Language*, (59:4), pp. 457-474.
- Böhme, R., and Köpsell, S. 2010. "Trained to Accept?: A Field Experiment on Consent Dialogs," In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, New York, NY, USA, pp. 2403-2406.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Behaviors in Users," *MIS Quarterly*, (Forthcoming).
- Bravo-Lillo, C., Cranor, L., Komanduri, S., Schechter, S., and Sleeper, M. 2014. "Harder to Ignore? Revisiting Pop-up Fatigue and Approaches to Prevent It," In: 10th Symposium

- On Usable Privacy and Security (SOUPS 2014), USENIX Association, Menlo Park, CA, pp. 105-111.
- Bravo-Lillo, C., Komanduri, S., Cranor, L. F., Reeder, R. W., Sleeper, M., Downs, J., and Schechter, S. 2013. "Your Attention Please: Designing Security-Decision UIs to Make Genuine Risks Harder to Ignore." Paper presented at the Proceedings of the Ninth Symposium on Usable Privacy and Security Newcastle, United Kingdom.
- Chen, S., and Chaiken, S. 1999. "The Heuristic-Systematic Model in Its Broader Context," in *Dual-Process Theories in Social Psychology*, S. Chaiken and Y. Trope (eds.), Guilford Press: New York, NY, US, pp. 73-96.
- 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.
- Gallagher, S. 2016. "Officials Blame "Sophisticated" Russian Hackers for Voter System Attacks," *Ars Technica* (available at <http://arstechnica.com/security/2016/08/officials-blame-sophisticated-russian-hackers-for-voter-system-attacks/>).
- Ghysels, E., Santa-Clara, P., and Valkanov, R. 2005. "There Is a Risk-Return Trade-Off after All," *Journal of Financial Economics*, (76:3), pp. 509-548.
- Goodin, D. 2016. "It's 2016, So Why Is the World Still Falling for Office Macro Malware?," *Ars Technica*).
- Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems*, (28:2), pp. 203-236.
- Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., and Weinmann, M. 2016. "How Is Your User Feeling? Inferring Emotion through Human-Computer Interaction Devices," *MIS Quarterly*, (forthcoming).
- Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., and Eargle, D. 2016. "More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable," *Information Systems Research*, (Articles in advance).
- Jensen, A. R. 2006. *Clocking the Mind: Mental Chronometer Individual Differences*, Elsevier: Amsterdam, Netherlands.
- 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.
- Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, (34:3), pp. 549-566.
- Kahneman, D., and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica: Journal of the Econometric Society*, pp. 263-291.
- Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal*, (25:5), pp. 433-463.
- McDonnell, J. V., Martin, J. B., Markant, D. B., Coenen, A., Rich, A. S., and Gureckis, T. M. 2012. "Psiturk (Version 1.02) [Software]," New York University (available at <https://github.com/NYUCCL/psiTurk>).
- Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology: A Sourcebook*, J. T. Cacioppo and R. E. Petty (eds.), Guilford: New York, pp. 153-176.



- Schechter, S. E., Dhamija, R., Ozment, A., and Fischer, I. 2007. "The Emperor's New Security Indicators," In: Security and Privacy, 2007. SP'07. IEEE Symposium on, IEEE, Berkeley, CA, pp. 51-65.
- Schneier, B. 2011. "Schneier on Security: Details of the RSA Hack," in *Schneier on Security*.
- Steelman, Z. R., Hammer, B. I., and Limayem, M. 2014. "Data Collection in the Digital Age: Innovative Alternatives to Student Samples," *MIS Quarterly*, (38:2), pp. 355-378.
- Sunshine, J., Egelman, S., Almuhiemedi, H., Atri, N., and Cranor, L. F. 2009. "Crying Wolf: An Empirical Study of SSL Warning Effectiveness," In: Proceedings of the 18th conference on USENIX security symposium, Montreal, Canada, pp. 399-416.
- Trumbo, C. W. 2002. "Information Processing and Risk Perception: An Adaptation of the Heuristic-Systematic Model," *Journal of Communication*, (52:2), pp. 367-382.
- Vance, A., Anderson, B. B., Kirwan, C. B., and Eargle, D. 2014. "Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG)," *Journal of the Association for Information Systems*, (15:10), pp. 679-722.