12-15-2019

Effects of emotional appeals on phishing susceptibility

Chuan Annie Tian

Matthew L. Jensen

Effects of Emotional Appeals on Phishing Susceptibility

Chuan (Annie) Tian[1]
MIS Division, University of Oklahoma,
Norman, OK, USA

Matthew L. Jensen
MIS Division, University of Oklahoma,
Norman, OK, USA

ABSTRACT

The heightened sophistication of phishing attacks results in billions of dollars of financial losses, loss of intellectual property, and reputational damage to organizations. Unlike most studies on phishing that utilize a strict cognitive approach, this study attempts to explore phishing susceptibility with an emotional lens. Using an integrated perspective of emotion, we build on the Affective Information Model (AIM) to predict effects from valence (positive vs. negative), certainty (certain vs. uncertain), and arousal (high arousal vs. low arousal) on phishing susceptibility. We test our hypotheses using a mock phishing experiment (N = 474) and demonstrate that messages inducing positive valence and uncertainty result in higher phishing susceptibility. This study contributes to phishing literature by illuminating the critical role that emotion plays in inducing recipients' susceptibility in their processing of phishing messages.

Keywords: Affect, Emotion, Affect Infusion Model, Phishing, Phishing Susceptibility, Valence, Certainty, Arousal

[1] Corresponding author: Chuan.Tian-1@ou.edu

INTRODUCTION

Digital communications are often exploited by cyber criminals to take advantage of individuals and organizations (Jensen et al. 2017). One of the most common techniques for defrauding others is phishing, whereby phishers attempt to steal confidential information, compromise networks, or spread malware by disguising malicious messages as legitimate communication. If individuals respond to a phishing message by clicking on links or opening attachments, they can not only compromise their own information security, but also imperil that of their organization. Consequences of phishing attacks can be steep with financial and intellectual property losses, damage to reputation, and fines and other legal penalties (Hong 2012). Phishing attacks can range from unsolicited requests targeting large numbers of unsuspecting victims to more hazardous threats such as tightly targeted spear-phishing campaigns. According to the Internet Crime Complaint Center (IC3) of Federal Bureau of Investigation (FBI), the number of phishing attacks has been surging with total estimated losses exceeding $3 billion and victims across the globe (FBI 2016).

Despite significant investments in automated screening, warning and reporting systems, and individual training, individuals remain susceptible to phishing attacks (AT&T Cybersecurity 2019). In response, researchers have begun investigating why individuals are so susceptible to phishing attacks. Scholars have uncovered individual differences (e.g., perceptions of risk) that increase the chance certain individuals will respond to phishing messages (Vishwanath et al. 2011; Wang et al. 2016; Wright and Marett 2010). Others have investigated how appearance, content, and layout constitute a more enticing message (Abbasi et al. 2010; Luo et al. 2013). Still others have uncovered techniques phishers use to more effectively coerce or persuade recipients to comply with message requests (Goel et al. 2017; Wright et al. 2014).

Although past inquiries have added to what is known about susceptibility, they ignore a potentially critical reason individuals fall for phishing messages. Past research has been dominated by cognitive theoretical perspectives explaining susceptibility. Affective processes, which can induce action in almost any circumstance, have been largely ignored in phishing research. For example, phishing research has been highly dependent on persuasion theory because phishers' primary goal with their attacks is to gain recipients' compliance (Goel et al. 2017). But persuasion scholars have emphasized the critical role that affective processes play in the shaping and changing of attitudes and suggest that appealing to emotions constitutes a venerable source of leverage in achieving persuasion (DeSteno et al. 2004). Even phishing research that has narrowly explored the use of affect in phishing messages has uncovered strong effects for content that promotes liking (Wright et al. 2014) or fear (Workman 2008).

To increase understanding about what contributes to phishing susceptibility, we systematically explore the role of affect in phishing messages. Drawing on an integrative view of emotion, we explore the effect of valance, certainty, and arousal on phishing susceptibility. Using the Affective Infusion Model (AIM; Forgas 1995), we hypothesize effects for each affective dimension on phishing susceptibility. We test our hypotheses using a field experiment with mock phishing attacks and offer implications of our findings for theory and practice.

THEORETICAL BACKGROUND

Bagozzi et al. (1999) refer to emotion as a subjective state arising from consistent or idiosyncratic cognitive appraisal of the events or perceptions. But other scholars (e.g., Dantzer 1989) conceive of emotions as a subjective representations of experience encompassing motivational and visceral factors and ignore cognition. In correspondence with this definitional division, two streams of emotional paradigms emerged, which are embodied respectively by

Russel's (2003) Circumplex Model and Scherer's (2005) Appraisal Theory. The Circumplex Model distinguishes emotions based on two universal and primitive perspectives: *valence* (positive vs. negative) and *arousal* (activation vs. deactivation), and distinctive emotions are mapped into the four quadrants at the intersection of these dimensions. Appraisal Theory, however, is rooted in the nuanced cognitive processes precipitating emotions and suggests emotional reactions as a consequence rather than the antecedent of an individual's appraisal of environmental stimuli (Scherer et al. 2001). Appraisal Theory also emphasizes the role of valence in its conceptualization, but also forwards the degree of *certainty* of outcome (certain vs. uncertain) as another core dimension governing how emotion arises (Bagozzi 1992).

To build theorizing on how phishing messages elicit distinct emotions to elevate or reduce phishing vulnerability, we embrace an integrative view of emotion and consider effects of valence, certainty, and arousal. The integrated view concerns both the physiological and a cognitive perspective when individuals respond to emotion-stimulating environments or events (Schachter and Singer 1962). The integrated view casts emotion generation by combining affective and cognitive process, suggesting they are mingled, synthesized, and interdependent (Solomon 1993). More specifically, affective processes can incorporate cognitive appraisal and interpretation of events, while rational processes are not completely detached and shielded from emotional feeling and experiences in one's information processing.

Emotions, Persuasion, and Phishing Susceptibility

Consistent with an integrated view, the AIM (Forgas 1995) suggests that affective and cognitive processes are mingled in interpreting environmental stimuli. Affect infusion is the process by which "affectively loaded information exerts an influence on and becomes incorporated into the judgmental process, entering into the judge's deliberations and eventually

coloring the judgmental outcome" (Forgas 1995, p. 39). Similar to the theoretical foundations of past phishing susceptibility research (Goel et al. 2017; Wright et al. 2014), the AIM is a theory of persuasion and explores attitude change and compliance with requests. Although emotions may be spontaneous or the result of appraisal, AIM argues that they are likely to be included in decisions through one of two routes: Affect-as-information or affect priming. The affect-as-information is associated with a heuristic information processing strategy and describes situations where affect is considered alongside other inputs during judgment (often subconsciously) (Forgas 1995). For example, along with superficial cues, one's favorable mood may increase preference for one option over another. Affect priming is associated with a more substantive, deliberate information processing strategy. As information processing becomes more atypical and complex, affect will more strongly influence information processing and subsequent action (Forgas 1995).

Prior phishing research has suggested that affect can play an important role in increasing susceptibility. For example, inducing fear in phishing recipients has been shown to be an effective way to achieve compliance with requests in messages (Workman 2008). For example, common attacks include phishers purporting to be authoritative senders and threatening severe consequences (e.g., account closure, fines and fees, data loss) if recipients do not immediately comply with message requests. Other work has demonstrated the power of positive affect (e.g., liking) as the impetus for complying with phishing requests (Wright et al. 2014) and suggested that people's tendency to respond to those they know and like dominate other forms of social persuasion. Still other work demonstrated the effects fear of loss and hope of gains have on phishing susceptibility and emphasized contextualization of the persuasion attempt embedded within the phishing message (Goel et al. 2017). Prior research has clearly demonstrated how

affect can play a prominent role in altering susceptibility to persuasive messages in general (Griskevicius et al. 2010) and with phishing messages in particular (Goel et al. 2017; Wright et al. 2014). However, the theoretical examinations of phishing susceptibility have largely ignored the role of affect and instead favored approaches based in cognition. Therefore, in this research we systematically address the role of affect in phishing susceptibility.

HYPOTHESIS DEVELOPMENT

Whether affect serves as an informational input to heuristic processing or as priming for more deliberate, systematic processing (as predicted by the AIM), previous studies have argued that emotion occupies a critical role in framing communication to increase message effectiveness (Nabi 2003). For example, emotions evoked by marketing messages can supplement and reinforce attempts at persuasion using other techniques (e.g., scarcity and social proof) (Griskevicius et al. 2010). As in these communication venues, emotional appeals in phishing messages motivate receivers to seek out and maintain circumstances that elevate their mood and avoid circumstances that might sour it. Furthermore, prior research has shown that in persuasion attempts aside from phishing, effects from emotional appeals might be additive (Griskevicius et al. 2010). Therefore, phishing messages that evoke emotion in addition to cognitive persuasive appeals (e.g., scarcity and social proof) are likely to be more compelling than messages that rely solely on cognitive appeals.

> *H1. Phishing messages eliciting emotions result in higher phishing susceptibility than those not eliciting emotions.*

In rational decision making, scholars have repeatedly demonstrated a negativity bias as evidenced by greater attention and more decision weight given to negative information or events than to positive or neutral information or events (Baumeister et al. 2001). This phenomenon is thought to occur because negative information is more salient, losses are more keenly felt than

gains, and the ease of negative differentiation (Rozin and Royzman 2001). Thus, one might conclude that phishing emails evoking a negative valence might be more effective than positive. However, the effects of emotion are more nuanced.

The primary reason for nuance is that phishing messages are deception. As opposed to messages in past research exploring the effect of valence on persuasion, statements by phishers are not legitimate threats against recipients' wellbeing; they are lies meant to fool the unsuspecting. For this reason, negative emotion can manifest complex effects on phishing susceptibility. On one hand, the AIM predicts that the infusion of negative emotion results in tightening of focus and increased monitoring. So, when a phishing message arrives with threats generating fear or anger, the recipient will likely be attentive to and focused on that message. But on the other hand, the AIM also predicts that with increased attention also comes increased scrutiny and more deliberative information processing (Forgas 1995). Therefore, any deception that accompanies or generates negative affect will likely be subjected to careful and systematic evaluation. Positive affect informs us that "the situation is favorable and that little monitoring and processing effort is required" (Forgas 1995, p. 50). In research examining deception aside from phishing, individuals who were induced to a positive mood were more easily fooled than those with a negative mood inducement (Forgas and East 2008). We expect the same to hold for deception in phishing messages.

> *H2. Phishing messages eliciting negative emotions result in lower phishing susceptibility than positive emotions.*

Aside from the valence, another primary dimension characterizing emotions is certainty (Smith and Ellsworth 1985). For example, joy and anger indicate a high degree of certainty, but hope and fear both indicate a low degree of certainty. Uncertainty derives from unpredictable opportunities or threats and orients those experiencing such emotions toward the source of the

contingency (Fiske 2018). Such narrowing of focus to the contingency rather than on the legitimacy of the message (especially if the contingency is trivial such as opening an attachment or clicking on a link) is likely to lead to higher susceptibility. Whether to avoid suffering negative consequences or to enjoy positive consequences, individuals will be motivated to escape the ambiguity and will be more likely to perform the requested the action (Kramer 1999).

H3. Phishing messages eliciting low-certainty emotions result in higher phishing susceptibility than high- certainty emotions.

Different from valence and certainty, arousal is the physiological and psychological state of being stimulated and activated toward a specific perception of stimuli (Russell 1980). When individuals are in an activated state, they are better able to encode and recall information (Bolls et al. 2001) and are alert and motivated to act (Lang 1995), but their attention narrows to the cause of the activation (Kapp et al. 1992) and impulsivity may also increase (Bagozzi et al. 1999). Thus, for the purpose of detecting phishing emails, arousal may exhibit competing effects.

To disentangle competing effects, we argue that the level of arousal becomes salient. With low level of arousal, heuristic, cursory information processing is likely, and individuals will not devote sufficient scrutiny to messages to detect incoming phishing. But with a moderate level of arousal, individuals will likely experience many of the effects of arousal that should increase ability to detect phishing. For example, the AIM predicts that higher motivation and alertness will contribute to more substantive information processing (Forgas 1995), which would result in more scrutiny being directed at a suspicious message. However, if arousal is very high, individuals will be unable to concentrate on incoming messages and will short circuit deliberative processing in favor of more impulsive judgement. Under such conditions, phishing messages may be more likely to slip through. Deception detection literature has shown similar

non-linear relationships between motivation and deception detection accuracy (George et al. 2014). We expect a similar relationship between arousal and phishing susceptibility.

H4. Phishing messages eliciting moderate arousal result in lower susceptibility than low arousal.

METHODOLOGY

We conducted a randomized experiment that used a mock phishing campaign to test our hypotheses. Those who volunteered participants in the experiment completed a pre-survey that discussed phishing, common ways to detect attacks, and gathered control variables that were included in the analysis. We then worked with the university IT security department to deliver mock phishing emails to participants' actual inboxes. The experiment design followed a 2 (valance: positive vs. negative) × 2 (certainty: certain vs. uncertain) × 2 (arousal: moderate vs. low) full factorial design. We designed a base phishing message and then manipulated it according to valance, certainty, arousal treatments.

Participants

Participants were recruited from a Midwest University introductory information systems class that is required for all business and several non-business majors. A total of 474 participants completed the pre-survey and were included in our sample. Indicating their suitability as participants, all participants used email, a total of 50% of participants reported knowing someone who had fallen for a phishing attack, and 30% reported coming close to falling for a phishing attack themselves.

Stimulus Materials

The baseline message along with the message manipulations for valence, certainty, and arousal are shown in Table 1. Valence was manipulated with purported gains versus losses as

well as positive versus negative language. Certainty was manipulated likelihood of the charge/refund. Arousal was manipulated by the dollar amount of the charge/refund.

Table 1. Message Manipulations.

[School Logo] Dear [School Name] Student, Your billing statement is now available. Please login to verify the balance in your Bursar account. [School Name] Bursar Office © Copyright 2019	[School Logo] Dear [School Name] Student, This is to inform you of pleasant *(unpleasant)* news that the Bursar Office discovered a software error and has issued a refund *(charge)* in the amount of $115.80 **[$463.20]** for overpayment *(underpayment)* for the Spring 2018 semester. Please login to your Bursar account to check the details of the new refund *(new charge)*. [School Name] Bursar Office © Copyright 2019	[School Logo] Dear [School Name] Student, This is to inform you the Bursar Office is conducting an investigation into a software error that may have resulted in students being overcharged *(undercharged)* for Spring 2018 semester. We hope *(are concerned)* that this investigation will result in a refund *(charge)* in the amount of $115.80 **[$463.2]** to you. Please login to your Bursar account to check your eligibility for the potential refund *(liability for the potential charge)*. [School Name] Bursar Office © Copyright 2019
Baseline Message	High Certainty *(valence treatment)* **[arousal treatment]**	Low Certainty *(valence treatment)* **[arousal treatment]**

Outcome and Control Variables

To measure phishing susceptibility, we used click throughs, which is coded as 1 if the subject clicks the link embedded in the phishing message and 0 if not. Click throughs are an objective measure that has been used in previous phishing research (Wright et al. 2014). Previous literature has also suggested several individual factors that may impact phishing susceptibility (Jensen et al. 2017). Therefore, we included them in our study as control variables. First perceived internet risk captures perceptions about the jeopardy of interacting and conducting business online (Jarvenpaa et al. 1999). Second, we gathered propensity to trust (Pavlou and Gefen 2004). Finally, we captured internal and external computer self-efficacy (Thatcher et al.

2008). Measurements properties of control variables met satisfactory levels, therefore we created summated scales and included them in the analysis.

RESULTS

Of the 474 participants, 76 (16%) of them clicked on the embedded link in the phishing messages. Response rates are sown in Table 2.

Table 2. Phishing Message Response Rate

Valence	Certainty	Arousal	N	Responses	Response Rate (%)
No Emotions			30	5	.17
Positive	Certain	High Arousal	52	8	.15
		Low Arousal	80	12	.15
	Uncertain	High Arousal	50	15	.30
		Low Arousal	50	12	.24
Negative	Certain	High Arousal	55	5	.09
		Low Arousal	50	4	.08
	Uncertain	High Arousal	55	9	.16
		Low Arousal	52	6	.12

To test H1, we conducted a logistic regression with emotions (no emotions = 0; emotions = 1) and other control variables as predictors and click throughs as the outcome variable. The results of the analysis are displayed in Table 3. The emotions variable failed to significantly influence click throughs, therefore H1 was not supported.

Table 3. Results of Logistic Regression with Emotion

Variable	B	S.E.	Wald	Df	Sig.	Exp(B)
Emotions	.062	.392	.025	1	.874	1.064
Risk	.038	.111	.117	1	.732	1.039
Trust	.072	.103	.487	1	.485	1.075
SE Internal	-.002	.107	.000	1	.988	.998
SE External	.214	.140	2.330	1	.127	1.238
Constant	-3.465	1.083	10.242	1	.001	.031

To test H2-H4, we conducted an additional logistic regression, but excluded the control condition to focus on messages that induced some kind of emotion. Valence (positive = 1; negative = 0), certainty (certain = 1, uncertain = 0), arousal (moderate arousal = 1, low arousal =

0) joined the other control variables as predictors and click throughs was the outcome variable. The results of the analysis are displayed in Table 4.

Table 4. Results of Logistic Regression with Valence, Certainty and Arousal.

Variable	B	S.E.	Wald	Df	Sig.	Exp(B)
Valence	.766	.282	7.371	1	.007	.465
Certainty	-.651	.282	5.325	1	.021	1.917
Arousal	.307	.277	1.227	1	.268	1.360
Risk	.064	.123	.272	1	.602	1.066
Trust	.083	.115	.523	1	.470	1.087
SE Internal	-.017	.117	.021	1	.884	.983
SE External	.343	.160	4.601	1	.032	1.409
Constant	-4.447	1.162	14.652	1	<.001	.012

The analysis shows clear support for H2 and H3. Positive valance and uncertainty increased susceptibility to phishing attacks. However, the analysis fails to support H4 as no significant effect from arousal was detected.

DISCUSSION

This study provides several important contributions. First, despite the prevalence of emotional manipulation in phishing campaigns, little research has examined the effect of emotions on phishing susceptibility focusing instead on cognitive approaches. This work uses an integrated approach to emotion and demonstrates that inducement of emotion does, in fact, alter susceptibility. Although phishers often send threatening messages demanding compliance, our research revealed that positive valence (rather than negative) was much more effective in convincing recipients to click on the phishing link. This finding is in line with other phishing research suggesting that positively valenced techniques (e.g., liking) might be more dangerous that negative (e.g., authoritative demands) (Wright et al. 2014). Second, uncertainty also contributed to increased levels of susceptibility. We hypothesized that when individuals would encounter feeling involving uncertainty, they would attempt to escape it by acting. In this case,

uncertainty induced by phishing messages caused a greater portion of participants to click on the phishing link, potentially endangering themselves and their organizations.

Our two central findings suggest that individuals will be most susceptible to what scholars call challenge emotions: excitement, hope, anticipation (Beaudry and Pinsonneault 2010) These are emotions characterized by positive valence and uncertainty and represent a potential vulnerability against which individuals and organizations should defend. In examining affect infusion, scholars have noted that often when attention is called to the role of emotion in decision making, affect infusion sharply declines (Forgas 1995). Thus, instituting techniques for identifying affect infusion in phishing attacks may reverse the increase in susceptibility individuals exhibit. However, this implication requires additional research.

Despite their effectiveness, challenge emotions seem to be infrequently induced in actual phishing messages. Instead, phishers often threaten severe consequences if recipients do not take action. But if message recipients comply with phishing requests, they are promised a return to the status quo (e.g., "Sign in so you won't lose your data…"). Even though they are more effective, inducing challenge emotions can come with potential costs for phishers. When phishers attempt to persuade individuals to take action to maintain the status quo, there are no actions for phishers to take if message recipients comply with their requests. But if phishers induce a challenge emotion (e.g., hope, anticipation), there is an implied promise of reward that phisher may be unable or unwilling to provide. If the implied promise goes unfulfilled, the phisher's deception could be easily discovered.

REFERENCES

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker Jr, J. F. 2010. "Detecting Fake Websites: The Contribution of Statistical Learning Theory," *MIS Quarterly* (34:3), pp. 435-461.

AT&T Cybersecurity. 2019. "Confidence: The Perceptions Nad Reality of Cybersecurity Threats." Retrieved September 5, 2019, from https://www.alienvault.com/resource-center/analyst-reports/perception-reality-cybersecurity-threats

Bagozzi, R. P. 1992. "The Self-Regulation of Attitudes, Intentions, and Behavior," *Social Psychology Quarterly*).

Bagozzi, R. P., Gopinath, M., and Nyer, P. U. 1999. "The Role of Emotions in Marketing," *Journal of the Academy of Marketing Science* (27:2), pp. 184-206.

Baumeister, R. F., Bratslavsky, E., Finkenauer, C., and Vohs, K. D. 2001. "Bad Is Stronger Than Good," *Review of General Psychology* (5:4), pp. 323-370.

Beaudry, A., and Pinsonneault, A. 2010. "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use," *MIS Quarterly*), pp. 689-710.

Bolls, P. D., Lang, A., and Potter, R. F. 2001. "The Effects of Message Valence and Listener Arousal on Attention, Memory, and Facial Muscular Responses to Radio Advertisements," *Communication Research* (28:5), pp. 627-651.

Dantzer, R. 1989. *The Psychosomatic Delusion: Why the Mind Is Not the Source of All Our Ills*. New York, NY: The Free Press.

DeSteno, D., Petty, R. E., Rucker, D. D., Wegener, D. T., and Braverman, J. 2004. "Discrete Emotions and Persuasion: The Role of Emotion-Induced Expectancies," *Journal of Personality and Social Psychology* (86:1), p. 43.

FBI. 2016. "Fbi Warns of Dramatic Increase in Business E-Mail Scams " Retrieved June 14, 2016, from https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

Fiske, S. T. 2018. *Social Beings: Core Motives in Social Psychology*. John Wiley & Sons.

Forgas, J. P. 1995. "Mood and Judgment: The Affect Infusion Model (Aim)," *Psychological Bulletin* (117:1), p. 39.

Forgas, J. P., and East, R. 2008. "On Being Happy and Gullible: Mood Effects on Skepticism and the Detection of Deception," *Journal of Experimental Social Psychology* (44:5), pp. 1362-1367.

George, J. F., Tilley, P., and Giordano, G. 2014. "Sender Credibility and Deception Detection," *Computers in Human Behavior* (35), pp. 1-11.

Goel, S., Williams, K., and Dincelli, E. 2017. "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems* (18:1), p. 22.

Griskevicius, V., Shiota, M. N., and Neufeld, S. L. 2010. "Influence of Different Positive Emotions on Persuasion Processing: A Functional Evolutionary Approach," *Emotion* (10:2), p. 190.

Hong, J. 2012. "The State of Phishing Attacks," *Communications of the ACM* (55:1), pp. 74-81.

Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. 1999. "Consumer Trust in an Internet Store: A Cross□Cultural Validation," *Journal of Computer□Mediated Communication* (5:2), pp. 0-0.

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Kapp, B. S., Whalen, P. J., Supple, W. F., and Pascoe, J. P. 1992. "Amygdaloid Contributions to Conditioned Arousal and Sensory Information Processing,").

Kramer, M. W. 1999. "Motivation to Reduce Uncertainty: A Reconceptualization of Uncertainty Reduction Theory," *Management Communication Quarterly* (13:2), pp. 305-316.
Lang, P. J. 1995. "The Emotion Probe: Studies of Motivation and Attention," *American Psychologist* (50:5), p. 372.
Luo, X. R., Zhang, W., Burd, S., and Seazzu, A. 2013. "Investigating Phishing Victimization with the Heuristic–Systematic Model: A Theoretical Framework and an Exploration," *Computers & Security* (38), pp. 28-38.
Nabi, R. L. 2003. "Exploring the Framing Effects of Emotion: Do Discrete Emotions Differentially Influence Information Accessibility, Information Seeking, and Policy Preference?," *Communication Research* (30:2), pp. 224-247.
Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp. 37-59.
Rozin, P., and Royzman, E. B. 2001. "Negativity Bias, Negativity Dominance, and Contagion," *Personality and Social Psychology Review* (5:4), pp. 296-320.
Russell, J. A. 1980. "A Circumplex Model of Affect," *Journal of Personality and Social Psychology* (39:6), p. 1161.
Russell, J. A. 2003. "Core Affect and the Psychological Construction of Emotion," *Psychological review* (110:1), p. 145.
Schachter, S., and Singer, J. 1962. "Cognitive, Social, and Physiological Determinants of Emotional State," *Psychological Review* (69:5), p. 379.
Scherer, K. R. 2005. "What Are Emotions? And How Can They Be Measured?," *Social Science Information* (44:4), pp. 695-729.
Scherer, K. R., Schorr, A., and Johnstone, T. 2001. *Appraisal Processes in Emotion: Theory, Methods, Research*. Oxford University Press.
Smith, C. A., and Ellsworth, P. C. 1985. "Patterns of Cognitive Appraisal in Emotion," *Journal of Personality and Social Psychology* (48:4), p. 813.
Solomon, R. C. 1993. "The Philosophy of Emotions," *Handbook of emotions* (2), pp. 5-13.
Thatcher, J. B., Zimmer, C., Gundlach, M. J., and McKnight, D. H. 2008. "Internal and External Dimensions of Computer Self-Efficacy: An Empirical Examination," *IEEE Transactions on Engineering Management* (55:4), pp. 628-644.
Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," *Decision Support Systems* (51:3), pp. 576-586.
Wang, J., Li, Y. H., and Rao, H. R. 2016. "Overconfidence in Phishing Email Detection," *Journal of the Association for Information Systems* (17:11), p. 1.
Workman, M. 2008. "Wisecrackers: A Theory□Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security," *Journal of the Association for Information Science and Technology* (59:4), pp. 662-674.
Wright, R. T., Jensen, M. L., Thatcher, J., Dinger, M., and Marett, K. 2014. "Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research* (25:2), pp. 385-400.
Wright, R. T., and Marett, K. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), pp. 273-303.