Examining the Relationship between Threat and Coping Appraisal in Phishing Detection among College Students

David J. Lemay[1], Ram B. Basnet[2*], and Tenzin Doleck[3]
[1]McGill University, Quebec, Canada
david.lemay@mail.mcgill.ca
[2]Colorado Mesa University, Colorado, USA
rbasnet@coloradomesa.edu
[3]University of Southern California, California, USA
tenzin.doleck@mail.mcgill.ca

Abstract

An important segment of information security research has focused on improving security protocols by encouraging protective behaviors in users of information technology. Intervention based research focused on changing users' responses to threat appraisals is informed by protection motivation theory (PMT). The present study proposed a model of the relationship between college students' threat perceptions, their level of anxiety and an adaptive coping response, here conceived as a behavioral intention to learn about phishing. Partial least squares structural equation modeling was used to empirically test a model of college users' response to perceived phishing threat and the relationship to their coping appraisal. We find that perceived detection threat negatively influenced detection efficacy and positively influenced anxiety, as expected. We did not find a relationship between detection efficacy and anxiety, nor did we find a positive relationship between anxiety and behavioral intention towards an adaptive coping response. The absence of a relationship between anxiety, efficacy, and behavioral intention is at odds with the main assumption of fear-based drive-reduction theories, that fear reduction induces protection motivation. Although we cannot rule out other coping responses such as emotion- or avoidance-based coping without experimental intervention, it remains unclear how distinct such coping behaviors are in practice.

Keywords: Threat and Coping Appraisal, Phishing, Phishing Detection, College Students, Behavioral Intentions

1 Introduction

Phishing is an important and well-studied field of cybersecurity [4, 6, 5, 7, 3]. Phishing is a form of attack that occurs when a malicious website impersonates a legitimate one in order to acquire sensitive information such as passwords, account details, financial and credit-card information. Phishing is a deception technique that utilizes a combination of social engineering and technology to gather sensitive and personal information by masquerading as a trustworthy person or business in an electronic communication such as SMS messages, emails and voice communication. A typical phishing attack makes use of spoofed emails that are made to look authentic and purported to be coming from legitimate sources such as financial institutions, e-commerce sites, etc., to lure users to visit fraudulent websites through links provided in the phishing email. The fraudulent websites are designed to mimic the look of a real company webpage.

Journal of Internet Services and Information Security (JISIS), volume: 10, number: 1 (February 2020), pp. 38-49
DOI: *10.22667/JISIS.2020.02.29.038*

*Corresponding author: Ram B. Basnet, Department of Computer Science and Engineering, Colorado Mesa University, Grand Junction, Colorado, USA, Tel: +1-970-248-1682, Web: `https://rambasnet.github.io`

By some estimates, security vulnerabilities cost industry upwards of five billion dollars annually in losses. However, the weakest link in the security chain is imputable not to the technological infrastructure but rather to human error. Thus, an important segment of information security research has focused on improving security protocols by encouraging protective behaviors in users of information technology. Intervention based research focused on changing users' responses to threat appraisals is informed by protection motivation theory (PMT). The rise of online phishing is one particular area that has garnered increasing attention as the internet has evolved into its central dominant place in business activity. Phishing involves using fraudulent emails to gain access to computer systems and otherwise compromise systems to defraud users by stealing information and other valuable assets.

The present study proposes a model of the relationship between college students' threat perceptions, their level of anxiety and an adaptive coping response, here conceived as a behavioral intention to learn about phishing.

2 Prior Phishing Studies

Prior phishing studies have found that email users rely on information cues such as the source, grammar and spelling, and semiotic features, including logos, titles, addresses, formatting and design features [42]. Studies have focused on how individuals recognize information cues in phishing emails and why some are fooled or fail to make a proper assessment [14, 16, 32, 33, 40, 41, 44]. Researchers have developed interventions to improve user phishing detection [24, 26, 25, 38] however researchers have not fully described the motivational processes involved in phishing detection [9, 12, 42]. Wang et al. [42] building on previous studies conceptualized coping adaptiveness as having both adaptive and maladaptive responses into the construct and included user anxiety into their extended parallel processing model.

Researchers in information security have employed a number of theories to explain individuals' reactions to fear appeals and appraisals from general deterrence theory to rational choice in addition to protection motivation theory. Boss et al. [9] critiqued the absence of fear-based manipulations in protection motivation studies that seek to understand how individuals respond on an affective level to perceived information security threats, due to a heavy focus on studies exploring the cognitive underpinnings of feel appraisals and control decisions. A PMT perspective recognizes the influence of non-cognitive dimensions on individual beliefs and behaviors including a concern for the affective dimensions and other motivational factors that help to explain the variegated number of responses to similar stimuli, or why given them same message do some individuals heed the warning and others do not change their behavior in the face of incontrovertible information. Wang et al.'s [42] extended parallel processing model (EPPM) is accommodated by PMT and the threat avoidance model of [31] which PMT subsumes as well [9, 35].

Drive reduction theories recognize emotions are strong motivators and negative emotions like fear and anxiety reduction are a prominent feature of number theories. Advocates claim EPPM is an extension of PMT in that it focuses on negative appraisals and justify the wholesale development of a separate theory when such bivalences in factors are explainable—and expected in cognitive appraisals. As Azjen [1] and Azjen and Fishbein [2] in the related area of reasoned action or planned behavior theories, optimal scaling poses an important methodological issue for modeling beliefs, attitudes, and intentions, as they are usually scored in unipolar fashion, when in reality they can form a bipolar continuum from negative evaluations on one end to positive evaluations on the other. Such bivalences can be accounted for through rescaling using simple linear transformations to represent subjective probabilities.

In recent years, cognitive theories have begun to account for the role of emotions and the affective dimension on individual appraisals and actions. Expectancy-value theories inherently recognize the multiplicity of drives that are integral to apprising behaviors and that these drives can operate both positively

and negatively. Such drives and their interrelations can be completely different between individuals and contexts because of the reflexivity which exists between the individual and the context (i.e., which results from interactions between individuals and situations). As recognized by Azjen and Fishbein [2], these factors and relationships are grounded in situational appraisals that are to a large extent context-dependent. Hence, persistent findings of low variance explained and low relationships between intentions and actions.

3 Protection Motivation Theory

Protection motivation theory grew out of drive-reduction research and its direct antecedent the parallel processing model [30] which posited two parallel processes, fear control and danger control though the model did not explain how emotion-based mechanisms give rise to the control processes [13]. Likewise, protection motivation has largely focused on the cognitive dimension [17]. PMT includes a range of coping responses that distinguish between adaptive and maladaptive responses [36, 37]. In their meta-analysis, Boss et al. [9] advanced a full nomological model of PMT stipulating operational definitions and hypothesized relationships for threat and coping appraisals grounded in Rogers' [37] original formulation. Thus, a threat appraisal consists of both vulnerability, the degree to which an individual beliefs the threat applies to his or her specific circumstances or the probability that the described threat will occur, and severity, the degree to which an individual beliefs the threat will cause consequential harm [9]. Increases in perceived severity, or conversely perceived vulnerability, lead to increases in protection motivation and concomitant increases in perceived fear, which as an emotional response, mediates the relationship between cognitive appraisals and coping behaviors. Individual differences including accuracy and self-efficacy increase protection motivation, whereas maladaptive rewards and response cost decrease it. Finally, increases in protection motivation induce security-related behaviors.

PMT studies generally vary the fear appeal condition [9], between a weak and a strong appeal, as fear is a precondition of fear drive-reduction studies of fear. Studies posit fear appeal as an antecedent, or a moderator to some factors, or even the whole model. However, studies have avoided using fear as direct antecedent as fear influences all aspects of the behavior model, and moderating influences are generally evaluated individually due to the infeasibility of testing fully moderated models.

PMT, similar to its direct antecedent the parallel-processing model, posits two main cognitive mediating processes: threat appraisal and coping appraisal. Wang et al. [42] identified three coping strategies namely task-based, emotion-based, and avoidance-based coping. Individual behaviors are classified on the adaptiveness of their response based on their assessments of rewards, the severity and their vulnerability of the threat, and their efficacy of response with respect to the costs of their coping behavior. Threat variables, self-efficacy and coping beliefs are most strongly associated with adaptive responses [17].

Floyd et al. [17] conducted the first meta-analysis of PMT reporting: "The mean overall effect size (d+= 0.52) was of moderate magnitude. In general, increases in threat severity, threat vulnerability, response efficacy, and self-efficacy facilitated adaptive intentions or behaviors. Conversely, decreases in maladaptive response rewards and adaptive response costs increased adaptive intentions or behaviors (p.407)". PMT was originally applied to health promotion and disease prevention; the meta-analysis demonstrated the general robustness of the PMT for studying health-related outcomes of individual and community interventions. More recently, PMT has been successfully applied to the field of information security [9].

4 Situating Protection Motivation Theory

Inherent in drive-reduction theories is the assumption that individual behaviors and cognitions are grounded in perceptual appraisals. However, the bias towards cognitive processes [9] involved in modeling relationships between beliefs and behaviors have tended to downplay the structuring role that situations play in forming individuals' beliefs and behaviors in terms of the affective and normative dimensions of human interactions as embedded in the social environment. A situated perspective recognizes the reflexive processes between individuals and activity contexts [20].

In their review of PMT, Floyd et al. [17] suggest a number of attributable sources of data heterogeneity across studies may be due to: "differences in ... perception[s] about the PMT factor, relative to the expected goal and suggested behaviors. In addition, population characteristics, such as age, may have contributed..." In the situated perspective, these differences are explainable as situational variations that influence individuals' interpretation of the activity, in other words, their situational understanding in other words, their individual definition of situation. In this perspective, individual behaviors result from the interplay of their beliefs and actions within social and activity systems which generate their own frame of reference [19], that is, develop local meanings that are shared by the participants engaging in such social practices. Floyd et al. [17] provide two examples that illustrate the seemingly paradoxical findings when trying to account for the disconnect between individuals' intentions and actions.

"In the first example, when faced with the threat of skin cancer, the subjects consistently endorsed using sunscreen as a protective behavior, yet consistently rejected staying out of the sun as a protective behavior, both of which are standard recommendations. Perhaps "staying out of the sun" may have a higher response cost than "using sunscreen"... The same behavior was endorsed much more strongly depending on the purpose or goal (p.419)".

"The decision to take protective action is a positive function of severity because one must believe that there is some harm (e.g., lung cancer for smokers), and that one is vulnerable to this harm. These considerations must override the rewards, both intrinsic (e.g., bodily pleasure of inhaling) and extrinsic (e.g., peer approval). This appraisal of threat supplies the motivation to initiate the coping process. To decide to adopt the recommended coping response, one must believe that performing the coping response will avoid the danger and that one has the ability and will to perform the response. These considerations must outweigh the costs (e.g., withdrawal symptoms) of performing the coping response (p.420)".

Indeed, as noted by Floyd et al. ([17], p.420-1) PMT ought not be considered a rational appraisal process. An important motivational component is affective, unconscious and automatic, and involves self-beliefs and probability assessments which are subject to biases in reasoning.

PMT offers a mechanism for effective behavior change by inducing protective actions using threat appeals and inducing adaptive coping responses using rewards and teaching effective actions to minimize response cost. Research suggests that sustaining intentions and adaptive responses may require follow-up interventions to address the gap between intentions and behaviors [17].

5 Fear Appraisals and Coping Adaptiveness in Phishing Detection

This study follows earlier work that examined the impact of phishing on users' online phishing detection [42]. Results showed that perceived detection efficacy increased coping adaptiveness but perceived phishing threat, partially mediated by phishing anxiety, decreased coping adaptiveness; coping adaptiveness positively mediated both detection effort and detection accuracy. Coping adaptiveness and detection effort appear differentially related to supporting effective detection. Wang et al. [42] model of perceived threat, phishing anxiety, and detection efficacy explained 28% of the variance in detection accuracy. Their study identified two three coping patterns, one task-based and the other emotion- and avoidance-

Table 1: Research hypothesis

Path	Relationship
PPT → DET	Negative
PPT → ANX	Positive
DET → ANX	Negative
ANX → BIN	Positive

based coping.

6 The Study Model

The present study attempts to model users' response to perceived threat and the relationship to their coping appraisal.

6.1 Preceived Threat

"The output is called perceived threat, defined as the subjective evaluation of the threat presented in the situation. It comprises two dimensions— perceived severity of the threat (i.e., the belief about the magnitude or significance of the threat and the gravity of its consequences) and perceived susceptibility to the threat (i.e., the belief about the probability of personally experiencing the threat)—which together determine the extent of perceived threat. ([42], p.381)"

6.2 Coping Appraisal

"The second appraisal, called the coping appraisal, deals with the individual's judgment of the ability to handle the threat and is measured by perceived efficacy, defined as cognitions about the effectiveness, feasibility, and ease with which a response alleviates or helps in avoiding a threat. It also comprises two dimensions—perceived response efficacy (i.e., the belief about how effective the response will be in averting a threat) and perceived self-efficacy (i.e., the belief about one's ability to carry out the response)—which together determine perceived efficacy ([42], p.381)"

Thus, we hypothesized that Phishing Anxiety (ANX) is influenced by Perceived Phishing Threat (PPT). PPT is influenced by perceived susceptibility to phishing attacks (SUS) and perceived severity of phishing victimization (SEV). Phishing detection efficacy (DET) and anxiety (ANX) influence behavioral intentions to learn about phishing (BIN) as an adaptive coping response. Table 1 summarizes the main path relationships tested. The first three hypotheses were derived from [42], and we proposed the fourth hypothesis based on our reading of the literature.

7 Method

7.1 Participants and Procedure

Participants included 72 computer science students from a southwestern college in the US. All participants voluntarily agreed to participate in the research. The convenience sample included 13 females and 59 males. Participants' average age was 22.79 years (SD=5.89). In terms of year of study, 14 were Freshman, 16 were Sophomore, 11 were Junior, and 31 were Senior.

Table 2: Model fit statistics

Measure	Values	Recommended Criterion
Average path coefficient (APC)	0.289, $P < 0.001$	Acceptable if $P < 0.05$
Average R-squared (ARS)	0.138, $P = 0.028$	Acceptable if $P < 0.05$
Average adjusted R-squared (AARS)	0.122, $P = 0.040$	Acceptable if $P < 0.05$
Average block VIF (AVIF)	1.151	Acceptable $if \leq 5$
Average full collinearity VIF (AFVIF)	1.202	Acceptable $if \leq 5$

7.2 Measures

A self-report questionnaire was used in the study. Along with demographic information, participants responded to statements related to the study measures: perceived phishing susceptibility, perceived phishing severity, perceived detection efficacy, phishing anxiety, and behavioral intention to learn about phishing.

Scales were gathered from previous literature. Perceived phishing susceptibility [42] was measured by a 2-item, 5-point Likert scale (1=Strongly Disagree; 5=Strongly Agree). Perceived phishing severity [42] was measured by a 2-item, 5-point Likert scale (1=Strongly Disagree; 5=Strongly Agree). Perceived phishing threat was modeled as a second-order construct consisting of perceived phishing susceptibility and perceived phishing severity. Perceived detection efficacy was measured by a 2-item, 5-point Likert scale (1=Strongly Disagree; 5=Strongly Agree). Phishing anxiety was measured by a 7-item, 5-point Likert scale (1=Strongly Disagree; 5=Strongly Agree). To measure behavioral intention to learn about phishing, we adapted the behavioral intention scale [39]; for each of the 3 items, students responded on a 5-point Likert scale (1=Strongly Disagree; 5=Strongly Agree).

8 Analysis and Results

Partial least squares structural equation modeling (PLS-SEM) [21] was used to empirically test the proposed research model: first assessing the measurement model and then the structural model. For the analyses, we used WarpPLS software [22, 23].

8.1 Measurement Model

As seen in Table 2, the data fit the model well [23].

We followed Kock's [23] guidelines for conducting PLS analyses. An evaluation of the measurement model is presented next. The measurement scale characteristics are presented in Table 3 Item reliability was established and the factor loadings which exceeded 0.70 are presented in Table 3. Furthermore, composite reliability coefficients of the measures exceeded the threshold value of 0.70 (Table 3). Thus, construct reliability was established. All average variance extracted (AVE) values exceeded the recommended threshold value of 0.50 (Table 3); thus, convergent validity of the constructs was confirmed.

Discriminant validity was evaluated and verified using the Fornell-Larcker criterion [18]. Table 4 reveals that all the diagonal values are greater than the off-diagonal numbers in the corresponding rows and columns. Therefore, discriminant validity was established using the Fornell-Larcker criterion [18].

In sum, the psychometric properties of the measurement model were deemed to be adequate.

Table 3: Measurement scale characteristics

Construct	Items	Loadings	Composite reliability (CR) coefficients	Average variance extracted (AVE)
DET	DET1	0.956	0.955	0.914
	DET2	0.956		
PPT	LV_SUS	0.736	0.703	0.542
	LV_SEV	0.736		
ANX	ANX1	0.879	0.959	0.824
	ANX4	0.884		
	ANX5	0.879		
	ANX6	0.943		
	ANX7	0.951		
BIN	BIN1	0.899	0.937	0.833
	BIN2	0.909		
	BIN3	0.929		

Table 4: Discriminant Validity Check

	DET	ANX	BIN	PPT
DET	**0.956**	-0.246	0.129	-0.397
ANX	-0.246	**0.908**	-0.035	0.383
BIN	0.129	-0.035	**0.912**	0.065
PPT	-0.397	0.383	0.065	**0.736**

8.2 Structural Model

The path estimation results are illustrated in Figure 1. There were no multicollinearity concerns [23] as all VIF values were below the suggested threshold of 5. Moreover, predictive relevance (Q2) was analyzed and Q2 coefficient values were greater than zero, thus establishing an acceptable level of predictive relevance [23].

Table 5 summarizes the results of the hypotheses testing (which includes path coefficients (β) and path significance (p-value), including effect sizes (f^2)) which are required for assessing the structural model. It should be noted that f^2 values of 0.35, 0.15, and 0.02 indicate large, medium, and small effect sizes, respectively [10].

*We proposed that the link between would be positive, however, it was negative, therefore the fourth hypothesis is not supported.

Table 5: Hypothesis Testing

Path	Path coefficient (β)	P value	Effect size (f^2)	Result
PPT $\rightarrow$ DET	-0.43	$P < 0.01$	0.19	Supported
PPT $\rightarrow$ ANX	0.34	$P < 0.01$	0.13	Supported
DET $\rightarrow$ ANX	-0.14	$P = 0.057$	0.04	Not Supported
ANX $\rightarrow$ BIN	-0.25	$P < 0.01$	0.06	$NotSupported^*$

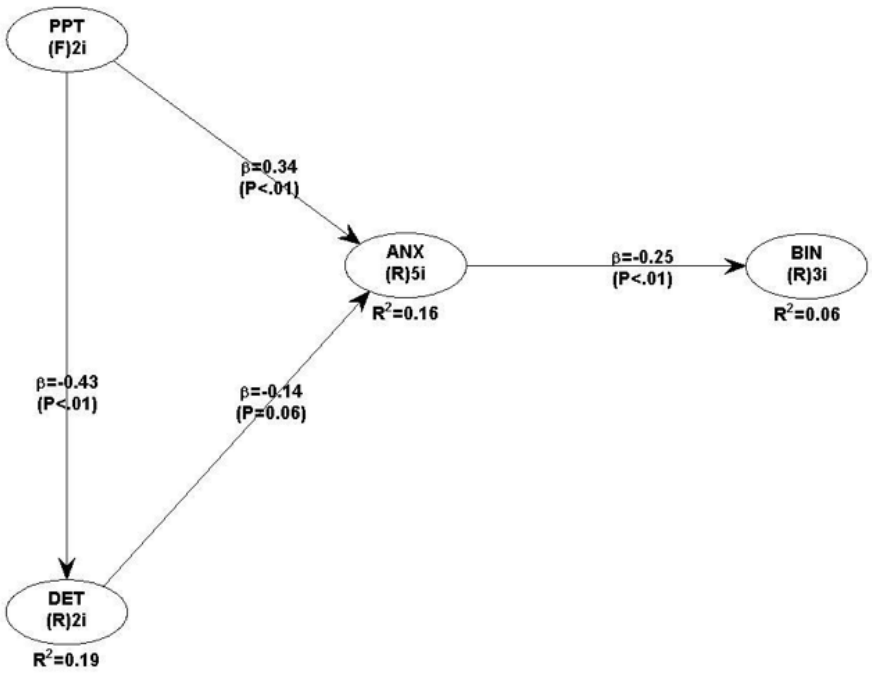

Figure 1: PLS Results

9 Discussion

The present study addresses individuals' coping behaviors regarding phishing email detection. In our study, perceived detection threat negatively influenced detection efficacy and positively influenced anxiety, as expected. We did not find a relationship between detection efficacy and anxiety, nor did we find a positive relationship between anxiety and behavioral intention towards an adaptive coping response. The absence of a relationship between anxiety, efficacy, and behavioral intention is directly at odds with the main assumption of fear-based drive-reduction theories, that is, that fear reduction induces protection motivation. However, we did not test a mediating effect for fear and we cannot rule out other coping responses such as emotion- or avoidance-based coping without experimental intervention. We did not conduct a fear appeal intervention as in [42]. However, it remains unclear how distinct such coping behaviors are in practice.

Whereas [42] distinguished task-, emotion-, and avoidance-based coping mechanisms, [31] argued two coping responses: "To reduce the threat, users have two options: problem-focused and emotion-focused coping. Problem-focused coping involves using safeguarding measures. Whether a safeguard is adopted is influenced by the safeguard's effectiveness and costs and users' self-efficacy. If no safeguarding measures exist to counter the malicious IT or the existing measures cannot completely reduce the threat, users are likely to perform emotion-focused coping, which helps them reduce the IT threat subjectively (p.85)". However, such a definition is hard to distinguish from an avoidance-based approach.

Evidently, emotion and avoidance based coping approaches are not clearly demarcated in practice. It is hard to deny that even avoidance behaviors can have both a positive and negative valence insofar as an individual may seek to effect a change of situational appraisal, as they can change their appraisal both by revising the importance of factors either up or down. Following control-value theory [34], if you can't change the situation, you can try to change the way you think about it. This amounts to a change in situational definition and is a powerful motivational response. Although in outward terms it might share features of avoidance or emotion-based coping, as the agent has not engaged in any behavior, it is arguably a problem- or task-focused response. To the extent that the stimuli evokes an emotional reaction, it is hard to disentangle that affective reaction from the cognitive appraisal and more importantly to discern a clear causal link between an action and an antecedent intention or affective state. As an absence of discernable outward behaviors does not suggest that the agent did not effect a change of state inwardly, we must recognize the bi-valence of affects, cognitions, and actions. Thus, it would seem that coping ought to be considered as a multidimensional construct that has both an affective, cognitive and performative dimension, since doing nothing can sometimes be the most adaptive behavior. Thus, it is likely that other moderating influences may explain the absence of direct relationships between anxiety, detection efficacy, and behavioral intention in our model. Indeed, given that the present study was conducted with university students as opposed to financial sector workers (the focus of much information security research), the stakes for phishing attacks are relatively lower, fear-based responses may be less salient as individuals have a greater range of coping mechanisms to deal with perceived phishing threats.

To some extent, phishing is afforded by the anonymous context of the internet. Internet scams such as email phishing prey on people's lack of technological proficiency or literacy, such that lack of efficacy for internet makes one vulnerable to scams and acts as a barrier to access to internet applications like email and file sharing by rising negative responses like fear or anxiety. We argue that the core attitudinal constructs ought not be considered uni-dimensional scale as and are best considered as a bi-modal continuum (Ajzen, 1991). Adaptive behaviors are largely determined by situations and contexts of use. In this case, perceived phishing threat had two very different responses, leading to heightened anxiety, and inversely related to perceived detection efficacy. Yet, heightened anxiety did not lead to behavioral intention for phishing detection. These two qualitatively different affective states likely have differential effects on beliefs and attitudes as well as behavioral intention, since the users have differing experiences of the technology: promoting efficacy or provoking anxiety. Given the wide disparities in modeling relationships in this area, and persistent findings pointing to the importance of situational and contextual variables in explaining individual behaviors, it is time to fully grapple with the significance of contextual-specificity. This is significant for job equity because research demonstrates that negative affect such as computer anxiety leads to a decreased level of computer or IT use in performing one's job decreasing performance [8, 11, 41, 42, 43]. To understand users' relationship to technology, we must move beyond strictly cognitive models to incorporate the affective dimensions but also the social and situational dimensions. Thus, it is important to consider the context of use in explaining technology acceptance behaviors, as individual reactions and uses of technology depend on situational factors that afford and constrain users' actions and beliefs. As Ajzen and Fishbein's [1, 2] theory of reasoned action makes explicit, situational variables influence the weighting and path relationships between attitudes and behaviors, and by extension, antecedent beliefs as well.

9.1 Limitations

The present study is limited by its use of a convenience sample, its cross-sectional design and its use of self-reports. The study's findings could be bolstered by the use of cluster-based and hierarchical sampling techniques, a longitudinal design, and the incorporation of additional measures for triangulating results [27].

9.2 Conclusions and Future Directions

PMT generally and phishing detection research specifically offers a novel area for research to study the relationship between affective and normative dimensions of technology use behaviors among individuals and social groups. As we have argued elsewhere [15, 28, 29], a fuller understanding of technology use, whether acceptance-oriented or coping-based, must be grounded in a theory of social behavior that accounts for the reflexive relationship between individual and society [20], as both the reproduction of the social order and social change are formed and influenced by interactions between individuals acting together for social ends. Thus, not only do subjective norms influence attitudes and behaviors, but social activities themselves are both afforded and constrained by individual perceptions and the social contexts of use [20].

References

[1] I. Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, December 1991.

[2] I. Ajzen and M. Fishbein. *Understanding attitudes and predicting social behavior*. Englewood Cliffs, 1980.

[3] R. Basnet and T. Doleck. Towards developing a tool to detect phishing urls: a machine learning approach. In *Proc. of the 2015 IEEE International Conference on Computational Intelligence & Communication Technology (CICT'15), Ghaziabad, India*, pages 220–223. IEEE, February 2015.

[4] R. Basnet, S. Mukkamala, and A. Sung. *Detection of Phishing Attacks: A Machine Learning Approach*. Springer, Berlin, Heidelberg, 2008.

[5] R. Basnet and A. Sung. Learning to detect phishing webpages. *Journal of Internet Services and Information Security (JISIS)*, 4(3):21–39, August 2013.

[6] R. Basnet, A. Sung, and Q. Liu. Rule-based phshing attack detection. In *Proc. of the 2011 International Conference on Security and Management (SAM'11), Las Vegas, Nevada, USA*, July 2011.

[7] R. Basnet, A. Sung, and Q. Liu. Learning to detect phishing urls. *International Journal of Research in Engineering and Technology*, 3(6):11–24, June 2014.

[8] A. Beaudry and A. Pinsonneault. The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, 34(4):689–710, December 2010.

[9] S. Boss, D. Galetta, P. Lowry, G. Moody, and P. Pollak. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4):837–864, June 2015.

[10] J. Cohen. *Statistical power analysis for the behavioral sciences (2nd ed.)*. Taylor & Francis Group, May 1988.

[11] D. Compeau and C. Higgins. Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2):189–211, June 1995.

[12] R. Crossler, A. Johnston, P. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. Future directions for behavioral information security research. *Computers & Security*, 32:90–101, February 2013.

[13] N. de Hoog, W. Stroebe, and J. de Wit. The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. *Review of General Psychology*, 11(3):258–285, September 2007.

[14] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In *Proc. of the 2006 SIGCHI Conference on Human Factors in Computing Systems (CHI'06), Montreal, Quebec, Canada*, pages 581—-590. ACM, April 2006.

[15] T. Doleck, P. Bazelais, and D. Lemay. Examining the antecedents of social networking sites use among cegep students. *Education and Information Technologies*, 22(5):2103–2123, September 2017.

[16] J. Downs, M. Holbrook, and L. Cranor. Behavioral response to phishing risk. In *Proc. of the 2007 Anti-Phishing Working Groups Second eCrime Researchers Summit (ECRIME'07), Pittsburgh, Pennsylvania, USA*, pages 37–44. ACM, October 2007.

[17] D. Floyd, S. Prentice-Dunn, and R. Rogers. A meta- analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2):407–429, July 2000.

[18] C. Fornell and D. Larcker. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1):39–50, February 1981.

[19] E. Goffman. *Frame analysis: An essay on the organization of experience*. Northeastern University Press, 1972.

[20] J. Greeno. Gibson's affordances. *Psychological Review*, 101(2):336–342, 1994.

[21] J. Henseler, G. Hubona, and P. Ray. Using pls path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems*, 116(1):2–20, February 2016.

[22] N. Kock, 2015. Retrieved from `http://www.warppls.com` [Online; accessed on February 10, 2020].

[23] N. Kock. Warppls 5.0 user manual. scripwarp systems. `http://cits.tamiu.edu/WarpPLS/UserManual_v_5_0.pdf` [Online; accessed on February 10, 2020], 2015.

[24] P. Kumaraguru. Phishguru: A system for educating users about semantic attacks, April 2009.

[25] P. Kumaraguru, S. S. A. Acquisti, L. Cranor, and J. Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2):1–31, June 2010.

[26] P. Kumaraguru, S. Sheng, and A. Acquisti. Lessons from a real world evaluation of anti-phishing training. In *Proc. of the 2008 Anti-Phishing Working Groups Second eCrime Researchers Summit (ECRIME'08), Atlanta, Georgia, USA*, pages 1–12. IEEE, October 2008.

[27] N. Leech and A. Onwuegbuzie. An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, 22(4):557–584, 2007.

[28] D. Lemay, T. Doleck, and P. Bazelais. "passion and concern for privacy" as factors affecting snapchat use: A situated perspective on technology acceptance. *Computers in Human Behavior*, 75:264–271, October 2017.

[29] D. Lemay, M. Morin, P. Bazelais, and T. Doleck. Modeling students' perceptions of simulation-based learning using the technology acceptance model. *Clinical Simulation in Nursing*, 20:28–37, July 2018.

[30] H. Leventhal. Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, 5:119–186, 1970.

[31] H. Liang and Y. Xue. Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), March 2009.

[32] J. Mohebzada, A. Zarka, A. Bhojani, and A. Darwish. Phishing in a university community: Two large scale phishing experiments. In *Proc. of the 2012 International Conference on Innovations Information Technology (IIT'12), Abu Dhabi, UAE*, page 249–254. IEEE, March 2012.

[33] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius. Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, 20(1):18–28, March 2012.

[34] R. Pekrun. The control-value theory of achievement emotions: Assumptions, corollaries, and implications for educational research and practice. *Educational Psychology Review*, 18(4):315–341, November 2006.

[35] L. Popova. The extended parallel process model. health education & behavior. *Health Education & Behavior*, 39(4):455–473, October 2012.

[36] R. Rogers. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1):93–114, September 1975.

[37] R. Rogers. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social Psychophysiology*, pages 153–176, 1983.

[38] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, and E. N. J. Hong. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proc. of the 3rd Symposium on Usable Privacy and Security (SOUPS'07), Pittsburgh, Pennsylvania, USA*, volume 229, page 88–99. ACM, July 2007.

[39] Venkatesh, Brown, Maruping, and Bala. Predicting different conceptualizations of system use: The competing roles of behavioral intention, facilitating conditions, and behavioral expectation. *MIS Quarterly*, 32(3):483–502, September 2008.

[40] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. Rao. Why do people get phished? testing individual

differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3):576–586, June 2011.

[41] J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. Rao. Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4):345–362, December 2012.

[42] J. Wang, Y. Li, and H. Rao. Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, 28(2):378–396, April 2017.

[43] J. Wilfong. Computer anxiety and anger: The impact of computer use, computer experience, and self-efficacy beliefs. *Computers in Human Behavior*, 22(6):1001–1011, November 2006.

[44] R. Wright, M. Jensen, J. Thatcher, M. Dinger, and K. Marett. Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, 25(2):385–400, June 2014.

Author Biography

David John Lemay is a postdoctoral fellow at McGill University, in Montreal, Canada. His research focuses on communicative and technology-mediated interaction.

Ram B. Basnet is an associate professor of Computer Science at Colorado Mesa University (CMU) in Grand Junction, USA. He received his BS in Computer Science from CMU and MS and PhD in Computer Science from New Mexico Tech. His research interests are in the areas of information assurance, machine learning, and computer science pedagogy.

Tenzin Doleck received his PhD from McGill University. He is currently a postdoctoral fellow at the University of Southern California in California, USA.