



## Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective

Ka Chung Ng, Xiaojun Zhang, James Y. L. Thong & Kar Yan Tam

To cite this article: Ka Chung Ng, Xiaojun Zhang, James Y. L. Thong & Kar Yan Tam (2021) Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective, Journal of Management Information Systems, 38:3, 732-764, DOI: [10.1080/07421222.2021.1962601](https://doi.org/10.1080/07421222.2021.1962601)

To link to this article: <https://doi.org/10.1080/07421222.2021.1962601>



© 2021 The Author(s). Published with license by Taylor & Francis Group, LLC.



[View supplementary material](#)



Published online: 07 Dec 2021.



[Submit your article to this journal](#)



Article views: 2228



[View related articles](#)






[View Crossmark data](#)



Citing articles: 2 [View citing articles](#)

# Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective

Ka Chung Ng <sup>a,b</sup>, Xiaojun Zhang <sup>b</sup>, James Y. L. Thong <sup>b</sup>, and Kar Yan Tam <sup>b</sup>

<sup>a</sup>Department of Management and Marketing, Faculty of Business, Hong Kong Polytechnic University, Hung Hom, Kowloon, HONG KONG; <sup>b</sup>Department of Information Systems, Business Statistics and Operations Management, School of Business and Management, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, HONG KONG

## ABSTRACT


A popular information security-related motivation theory is the Protection Motivation Theory (PMT) that has been studied extensively in many information security contexts with promising results. However, prior studies have found inconsistent findings regarding the relationships within PMT. To shed light on these inconsistent findings, we introduce the attitudinal ambivalence theory to open the black box within PMT. We tested our model on data collected from 1,383 individuals facing potential cyberattacks of their emails in a field experiment. The results of polynomial regression with response surface analysis showed that attitudinal ambivalence is generated from the opposition between an individual's evaluations of maladaptive rewards and social norms (i.e., descriptive norm and subjective norm). This attitudinal ambivalence, in turn, affects individuals' evaluations of their coping appraisal process and protection motivation, and ultimately protection behavior. We discuss the theoretical and managerial implications of identifying the determinants and outcomes of attitudinal ambivalence in the information security context. From a theoretical standpoint, our work contributes to the information security literature by incorporating attitudinal ambivalence, which arises from the intrapersonal and interpersonal appraisal processes, into PMT. From a practical standpoint, our work provides insights into designing effective fear appeals to avoid triggering attitudinal ambivalence and thus encouraging adoption of security protection behavior.


## KEYWORDS

attitudinal ambivalence theory; information security; protection motivation theory; two-factor authentication; maladaptive rewards; polynomial regression; response surface analysis; social norms; cybersecurity; security breaches

## INTRODUCTION

More and more companies are affected by cybersecurity breaches [9,35] that lead to compromised personal data [1,44,90] and violations of individuals' privacy [45,47]. Despite the fact that more and more individuals have become alert to cybersecurity threats, they are still often the weakest link in cybersecurity attacks [30]. According to an annual Cisco [21]'s cybersecurity report, a major target of cyberattacks is security awareness deficit among individuals who are prone to engaging in behaviors that compromise security, such as clicking malicious links in emails or websites. Hence, it is imperative to enhance individuals' cybersecurity awareness and motivate them to take actions against cybersecurity threats.

**CONTACT** James Y. L. Thong  [jthong@ust.hk](mailto:jthong@ust.hk)

 Supplemental data for this article can be accessed on the [publisher's website](#).

© 2021 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

Among the various theoretical lens adopted in the IS literature to examine cybersecurity threats, the protection motivation theory (PMT) is one of the dominant information security model explaining how individuals cope with and make decisions when facing cybersecurity threats (e.g., [28,51,60,65,79]). A core assumption of PMT is that if a threatening message causes fear, individuals will be motivated to engage in behaviors to reduce that fear because it is perceived as an unpleasant emotional state. PMT argues that a fear appeal will initiate threat and coping appraisal processes that affect individuals' motivation to engage in protection behaviors [12,83]. The threat appraisal process evaluates the severity of the threat, its possibility of occurrence, and the rewards resulting from not engaging in protection behaviors, whereas the coping appraisal process evaluates the effectiveness, difficulty and incurred costs of engaging in the recommended protection behaviors [73]. Both appraisal processes capture an individual's feelings and thoughts about cybersecurity threats and, therefore, can be viewed as intrapersonal processes. Social norms, which capture the influence of the majority (i.e., descriptive norm) or significant others (i.e., subjective norm), were later introduced into PMT [3,83] and can be viewed as the *interpersonal appraisal process*.

Despite the popularity of PMT, prior research has found inconsistent findings when PMT was used either as a complete or segmented theoretical framework to predict the motivation to engage in protection behaviors against cybersecurity threats. For example, some studies have found unsupported or even contradictory relationships in the threat appraisal process (e.g., [29,50]) and coping appraisal process (e.g., [86,94]). There are also inconsistent findings in studies that incorporate social norms into the PMT (e.g., [3]). To gain a more nuanced understanding of the inconsistent findings within PMT when situated in the information security context, we reviewed the number of supported/unsupported studies for each relationship proposed in PMT and presented the results in Table 1 (with details of the analysis and a summary of the inconsistent findings among PMT studies documented in Appendix A). On average, 50% (i.e., Perceived Severity: 21 out of 38 studies, Fear: 4 out of 9 studies) and 24% (i.e., Self-Efficacy: 11 out of 50 studies) of the studies did not support the relationships in the threat and coping appraisal processes respectively. Further, a significant number of studies did not support the relationships in the interpersonal appraisal process (e.g., [3]).

The inconsistent findings prompt us to reexamine the core assumption and the underlying mechanisms of PMT. PMT relies on the threat/fear appeal, a persuasive message that intends to scare individuals to become aware of the threat and help individuals form

**Table 1.** Unsupported PMT Relationships in Prior Studies

PMT Relationships	Percentages
<i>Threat-appraisal</i>	
Perceived Severity → Protection Motivation	55% (21 out of 38 studies)
Perceived Vulnerability → Protection Motivation	64% (25 out of 39 studies)
Fear → Protection Motivation	44% (4 out of 9 studies)
Maladaptive Rewards → Protection Motivation	58% (7 out of 12 studies)
<i>Coping-appraisal</i>	
Response Efficacy → Protection Motivation	25% (13 out of 51 studies)
Response Costs → Protection Motivation	25% (8 out of 32 studies)
Self-Efficacy → Protection Motivation	22% (11 out of 50 studies)
<i>Interpersonal-appraisal</i>	
Descriptive Norm → Protection Motivation	11% (1 out of 9 studies)
Subjective Norm → Protection Motivation	47% (8 out of 17 studies)

cognition of efficacy in dealing with the threat [65]. While a fear appeal can motivate individuals to engage in protection behavior, a simultaneously opposing force (e.g., maladaptive rewards or perceived benefits of not engaging in protection behaviors) can inhibit them from taking the recommended action. PMT assumes that individuals will take the recommended actions only if they think that the threats outweigh the maladaptive rewards. However, this assumption is generally an oversimplification of the real situation. More often than not, individuals could concurrently perceive similar levels (high or low) of security threat and maladaptive rewards. As an example, individuals may be eager to adopt protection behaviors because they are afraid of cyberattacks (e.g., [44]) or their friends recommend them to do so (e.g., [3]). At the same time, they may prefer not to do anything as installing and managing security software could be both time- and effort-consuming. Under these circumstances, individuals may feel “indecisive” toward the action of using security software. In this regard, we argue that fear appeal likely acts as a trigger of attitudinal ambivalence, a state in which individuals experience simultaneous positive and negative evaluations toward an attitude object [4], as it prompts individuals to evaluate different facets of the protection behavior. To the best of our knowledge, prior studies have not explicitly considered how attitudinal ambivalence can affect individuals’ behavior in response to cybersecurity threats. In light of this, we draw from the attitudinal ambivalence theory [4,68] to shed light on the inconsistent findings in the PMT literature and to gain a better understanding of what motivates individuals to engage in protection behaviors against cybersecurity threats.

The attitudinal ambivalence theory is relevant to the information security context, considering that the fear appeal is likely to invoke mixed feelings or beliefs among individuals. A growing body of literature [17,18,64,82] suggests the co-existence of positive and negative evaluations toward an object within an individual, inspiring us to introduce the concept of attitudinal ambivalence to the information security context. Specifically, we seek to understand the antecedents of attitudinal ambivalence and the behavioral outcomes after individuals experience attitudinal ambivalence. To better understand how attitudinal ambivalence is formed, we delve into the information security context where security awareness deficit among individuals is a major concern to identify important factors within PMT, that can cause attitudinal ambivalence. Several studies have documented that there is a tradeoff between security or usability and convenience, in which enhancement in security is always associated with an increase in inconvenience (e.g., [37]). We thus argue that maladaptive rewards, defined as any general rewards (intrinsic or extrinsic), such as time, effort, and pleasure, received by not adopting the security protection behaviors in PMT is the most salient factor that can give rise to attitudinal ambivalence when individuals process the fear appeal. Further, using polynomial modeling and surface response analysis, we will validate the key antecedents of attitudinal ambivalence within PMT [14,15,35,91].

Our study makes contributions to the information security literature. First, we incorporate attitudinal ambivalence as a potential theoretical mechanism into PMT to shed light on the inconsistent findings across previous PMT studies. We propose that fear appeal is a trigger of attitudinal ambivalence as it prompts individuals to evaluate different aspects of the protection behavior. The attitudinal ambivalence theory also helps us understand behavioral change when individuals experience conflicting views and/or feelings arising from the appraisal processes. It thus provides a new and alternative explanation for how PMT operates. Second, by incorporating both the intrapersonal and interpersonal appraisal

processes into PMT and examining their independent and interdependent roles in affecting attitudinal ambivalence, which in turn affects the coping appraisal process, we complement the existing nomological network of PMT. Third, we advance the fear-appeal perspective in information security research by identifying maladaptive rewards as an important contextual factor that gives rise to attitudinal ambivalence. We examine the potential antecedents of attitudinal ambivalence and its consequences when individuals encounter and process a fear-appeal, thus gaining insights into the effectiveness of fear appeal design in influencing individuals' protection motivation and behavior.

## THEORETICAL BACKGROUND

### *Protection Motivation Theory*

Rogers [72] developed PMT to explain how and why people are motivated to undertake health-related protection behaviors. Since then, there have been many extended versions of PMT to study individuals' responses to different types of threats in various contexts [19,79]. PMT focuses on the intrapersonal appraisal process that is divided into the threat and coping appraisal processes. The threat appraisal process generally involves perceived threat severity, threat vulnerability, fear, and maladaptive rewards, and the coping appraisal process involves response efficacy, self-efficacy, and response costs (e.g., [5,57]). Table 2 provides the definitions of key PMT constructs.

In the threat appraisal process, PMT argues that fear invoked by perceived threat severity and perceived threat vulnerability will motivate people to take protection behaviors [72]. It is important to note that PMT will hold only when a fear appeal is strong enough to make people aware of the threat and hence experience fear. This aligns with a key assumption of PMT in that protection motivation will only be aroused when people perceive that the threat is severe, likely to occur and can be coped [72]. Thus, it is crucial to apply fear-appeal in PMT studies. Further, the concept of maladaptive rewards is incorporated into PMT considering its important role in affecting the threat appraisal process (e.g., [12]).

Following the threat appraisal process is the coping appraisal process, during which people evaluate their capability of coping with the invoked threat by engaging in protection behaviors. In the coping appraisal process, people will follow the recommendation only when they think it is effective, simple, and will not incur more costs than benefits. In the

**Table 2.** Definitions of Key PMT Constructs (from Boss et al. [12])

Construct	Definition
Perceived threat severity	The degree to which an individual believes the threat will cause consequential harm.
Perceived threat vulnerability	The degree to which an individual believes the threat applies to his or her specific circumstances.
Fear	It represents a negatively valenced response to emotional, cognitive and physical danger. This response can be any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood.
Maladaptive rewards	Any general rewards (intrinsic and extrinsic) received by not adopting the protection behavior, such as time, effort and pleasure.
Response efficacy	The degree of perceived effectiveness of the recommended response.
Response costs	Any perceived costs incurred when taking the recommended action.
Self-efficacy	The degree of perceived capability people think they have in performing the recommended task.

information security context, PMT has been used to understand many protection behaviors, such as data backup, anti-malware software use, security policy compliance, internet security, and home computer security [3,19,52,89].

### ***Attitudinal Ambivalence Theory***

Traditionally, attitude is theorized to be unidimensional, i.e., the sum total of an individual's feelings and thoughts toward a specific object [87]. This unidimensional conceptualization of attitude ignores much richness and potential of the attitude construct, which may be multidimensional in reality [85]. Thompson et al. [85] reconceptualize attitude and propose the concept of *attitudinal ambivalence*. Attitudinal ambivalence is defined as a state when individuals tend to provide equally strong positive and negative evaluations toward attitude objects or things that individuals make a judgment about or have a feeling toward [84]. There are deviations in the literature about the definition of ambivalence, for example, cognitive ambivalence, attitudinal ambivalence, and emotional ambivalence [4,24]. In this paper, we choose not to differentiate between cognition and emotion as they are not independent but intertwined [4,23]. Ashforth et al. [4] indicate that ambivalence is a cognitive-emotional construct. According to Conner and Armitage [23], attitudinal ambivalence embraces both cognition and affect, and arises when either cognition or emotion, or both, clash. In line with Ashforth et al. [4], we consider both intention and behavior as the consequences of attitudinal ambivalence.

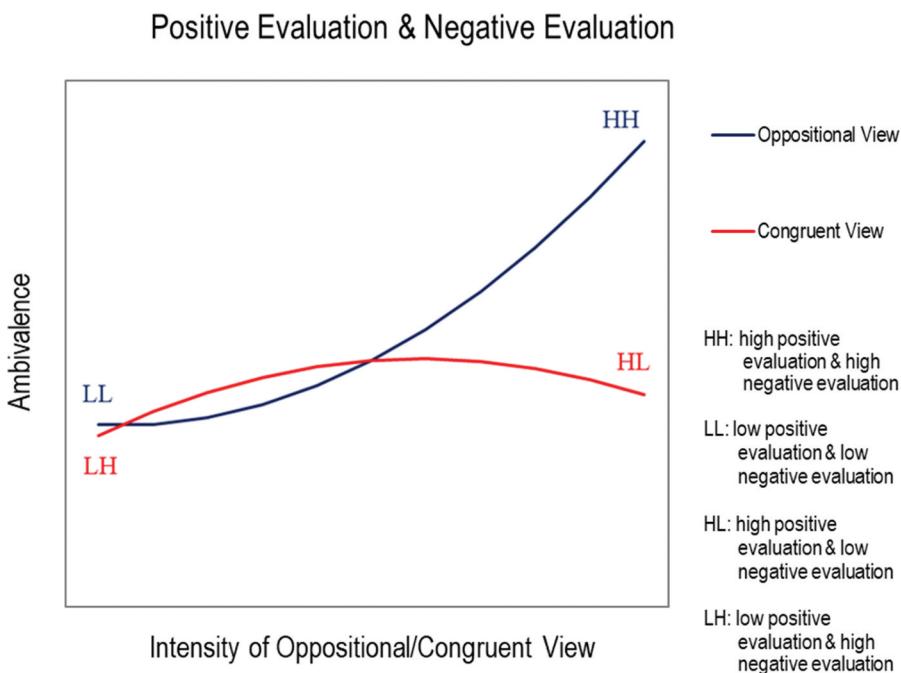
### ***Antecedents of Attitudinal Ambivalence***

Ashforth et al. [4] propose four major types of organizational triggers of attitudinal ambivalence based on the contextual root of oppositions. In line with their arguments, we argue that in the current context where security awareness deficit among individuals is a major concern, oppositions manifest when individuals face a fear appeal that invokes the recommended action after cognitively and emotionally assessing the threat in the fear appeal, leading to an experience of attitudinal ambivalence. Attitudinal ambivalence may arise from the competing forces of ones' own positive and negative evaluations, i.e., the intrapersonal process, as well as the discrepancy between ones' own thoughts and what others believe, i.e., the interpersonal process (e.g., [70,75]).

To better understand the formation of attitudinal ambivalence in the context of information security, we will investigate which facets of the protection behavior are evaluated simultaneously that can give rise to the experience of attitudinal ambivalence. Prior research has shown that security is a tradeoff with convenience [37,95]. For instance, the most common way for user authentication is to use a password, even though it is vulnerable to cyberattacks. An additional security layer has been proposed to supplement the standard password-only approach, which is referred to as two-factor authentication (2FA). This approach confirms the identity of a user through a combination of two different factors, e.g., a password and phone verification. With 2FA, security is strengthened, but at the same time, the use of the second factor necessitates extra effort and time. Hence, the role of maladaptive rewards or the benefit of saving time and effort by not engaging in protection behaviors is critical in the context of information security. Meanwhile, the goal of a fear appeal is to persuade individuals to engage in the protection behavior by making individuals

aware of the threat through the emphasis on the severity of the threat and the individuals' vulnerability toward the threat [52]. We thus presume that individuals will establish positive beliefs toward the protection behavior. However, maladaptive rewards will act as a negative force that deters individuals from engaging in the protection behavior. Therefore, individuals with high levels of maladaptive rewards are more likely to experience attitudinal ambivalence because maladaptive rewards are likely to be in conflict with other positive evaluations toward the protection behavior.

To better understand how attitudinal ambivalence is formed, it is not sufficient to identify only the competing or conflicting forces considering that these forces also manifest as different levels of positive and negative evaluations toward the protection behavior: 1) low levels of both positive and negative evaluations (labeled as *LL*), 2) high levels of both positive and negative evaluations (labeled as *HH*), 3) high level of positive evaluation with low level of negative evaluation (labeled as *HL*), and 4) low level of positive evaluation with high level of negative evaluation (labeled as *LH*). In general, attitudinal ambivalence will arise from *HH* and may also arise from *LL*, and likely to peak when the competing forces are at their strongest, i.e., when the levels of both positive and negative evaluations are at their highest. Besides, there should be low, or possibly no, attitudinal ambivalence arising from *HL* and *LH*, given that in both these cases, there is a dominant positive or negative evaluation. The formation of attitudinal ambivalence can be better explained by the *oppositional* and *congruent views* [32] that describe how attitudinal ambivalence is formed (see Figure 1). The *oppositional view* describes the scenario where the levels of positive and negative evaluations are similar, while the *congruent view* describes the scenario where the levels of positive and negative evaluations are at odds. The *oppositional view* is an increasing



**Figure 1.** Illustration of Different Levels of Positive and Negative Evaluations



function of attitudinal ambivalence as more intense conflicting forces should lead to more experience of attitudinal ambivalence. In the *congruent view*, it is a concave function (inverted U) of attitudinal ambivalence. This is because attitudinal ambivalence is unlikely to exist at both extremes (LH and HL), and will only arise when positive and negative evaluations start to be at odds. Although attitudinal ambivalence is mainly elucidated from the *oppositional view*, it is also crucial to look into the *congruent view*, which captures the nonlinear pattern of how attitudinal ambivalence is formed. Therefore, our paper incorporates both the *oppositional view* and *congruent view* in studying the antecedents of attitudinal ambivalence. In summary, delving into the different levels of positive and negative evaluations provides us with a fine-grained and comprehensive view of the antecedents of attitudinal ambivalence, which is largely missing from prior attitudinal ambivalence research.

### **Consequences of Attitudinal Ambivalence**

Prior studies have shown that attitudinal ambivalence is aversive [66] and can cause psychological discomfort among individuals when they are required to act on the conflicting thoughts, such as deciding whether to engage in protection behaviors against cybersecurity threats [39]. Owing to the unpleasant feelings, individuals are motivated to reduce the inconsistencies by using two approaches – *defense mechanism* and *coping mechanism* [4]. The defense mechanism, which is nonconscious and nonintentional, is used to “protect the people from excessive anxiety, whether the source of that anxiety be the perception of a disturbing external event or the presence of a disruptive internal psychological state” [26, p. 920]. The coping mechanism, which is conscious and intentional, is used to help people resolve the problem and/or alleviate the tension [4,26]. Both mechanisms are deployed to help resolve the anxiety and aversion caused by attitudinal ambivalence. Ashforth et al. [4] further classifies these two mechanisms into four possible responses to attitudinal ambivalence, i.e., *compromise*, *holism*, *avoidance*, and *domination*. In our study, we argue that individuals are more likely to adopt the domination mechanism to reduce attitudinal ambivalence toward protection behavior (see Appendix B for a discussion of why the other mechanisms do not apply in our context). Domination is widely used when individuals must choose between two opposing and mutually exclusive evaluations, such as engaging in or not engaging in protection behaviors. It can be a defense mechanism through which individuals nonconsciously amplify one side of the conflicting thought so that it outweighs the other side, and/or a coping mechanism through which individuals consciously commit to one side and ignore the other [4]. In the context of information security, we argue that domination is a defense mechanism as individuals will nonconsciously amplify the negative aspects of the protection behaviors due to biased systematic processing.

Unbiased systematic processing occurs when individuals thoroughly weigh all the conflicting thoughts to make the right decision [40]. In such a case, ambivalence is likely to increase because individuals will be struggling with the conflicting thoughts. Biased systematic processing, which involves less cognitive effort, is more likely to be used when individuals are struggling with conflicting views in making a decision [40]. According to the consistency theories, such as the *balance theory* [41] and the *cognitive dissonance theory* [33], people prefer consistency in their thoughts, feelings or behaviors because inconsistency is unpleasant. In this regard, prior research further argues that when individuals use



biased systematic processing, they nonconsciously amplify views/attitudes that are initially formed or strongly held [4,66]. In the context of information security, we argue that individuals will be nonconsciously prone to biased systematic processing in response to the large amount of cognitive resources consumed when experiencing attitudinal ambivalence. Besides, as individuals pay less attention to cybersecurity threats and lack the motivation to engage in protection behaviors, extant studies consider these individuals as the weakest link in cybersecurity [16,81]. Therefore, given that individuals' initial motivation to engage in protection behavior is likely to be low due to their lack of cybersecurity awareness, we argue that individuals resorting to biased systematic processing will focus more on the negative aspects of engaging in protection behaviors, such as viewing it as an ineffective and costly means to reduce attitudinal ambivalence. Specifically, these individuals will lean favorably toward response costs and unfavorably toward response efficacy, self-efficacy, and protection motivation.

## RESEARCH MODEL AND HYPOTHESES

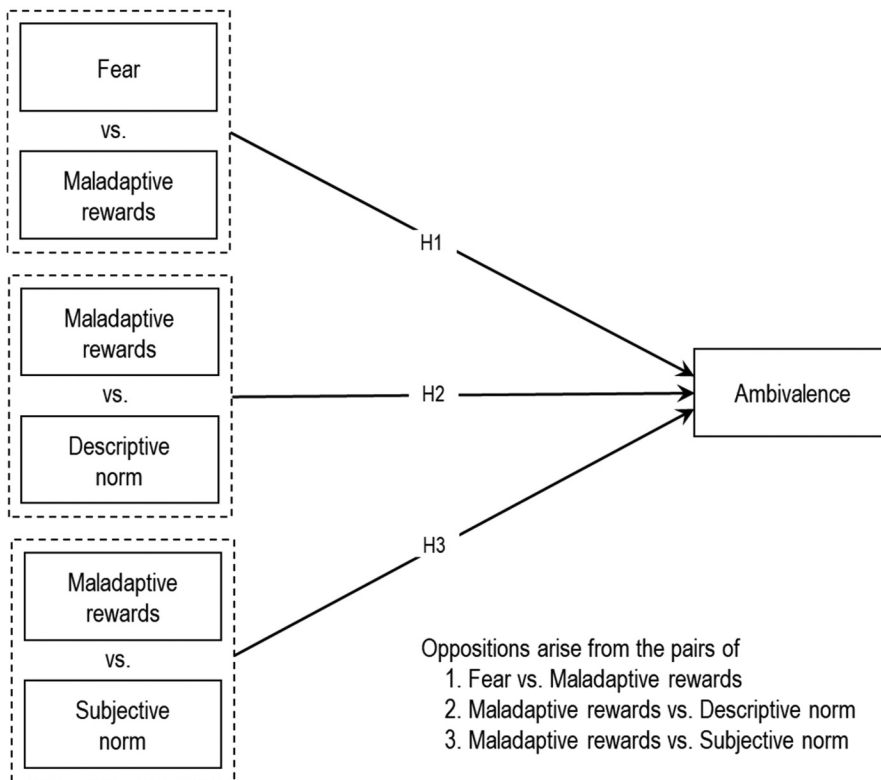
This research aims to reconcile the inconsistent findings in PMT by drawing from the attitudinal ambivalence theory. Specifically, we incorporate attitudinal ambivalence that is examined within and across the intrapersonal and interpersonal processes, and emphasize maladaptive rewards as a key driving force for attitudinal ambivalence. A fear appeal is designed with two parts: the first part showing some threatening message and the second part showing some efficacy arguments. PMT posits that individuals will first undergo the threat appraisal process, followed by the coping appraisal process. We argue that attitudinal ambivalence may arise when conflicting thoughts emerge from within the intrapersonal or threat appraisal process and/or from the interaction between the intrapersonal and interpersonal appraisal processes, e.g., sometimes an individual may change her own view to conform to those held by the majority or significant others. This ambivalent attitude will then affect the individual's formation of efficacy of the protection behavior and his/her ability in performing the behavior, when he/she processes the second part of the fear appeal. Hence, attitudinal ambivalence will arise before the coping appraisal process.

In light of the above arguments, we paired up several constructs within the threat appraisal process and between the threat appraisal and interpersonal appraisal process. We did not select constructs from the coping appraisal processes (i.e., response efficacy, response costs, self-efficacy) because we argue that attitudinal ambivalence will precede the coping appraisal processes, which is consistent with the temporal/causal sequence (i.e., individuals will undergo the threat appraisal first, followed by the coping appraisal) proposed in PMT. The paired constructs are selected to represent the conflicting views and are theorized as antecedents of attitudinal ambivalence. This approach of using paired constructs to represent antecedents of attitudinal ambivalence is consistent with prior studies (e.g., [75,80]). We considered pairs that include maladaptive rewards as important antecedents that give rise to attitudinal ambivalence. Specifically, we paired the constructs (fear, descriptive norm, and subjective norm) classified as positive evaluation (i.e., constructs that are positively related to protection motivation) with the construct (i.e., maladaptive rewards) classified as negative evaluation (i.e., construct that is negatively related to protection motivation). We did not consider perceived severity and perceived vulnerability because their effects would already be captured by fear. We chose only three pairs of

constructs as antecedents of attitudinal ambivalence because they are most likely to give rise to conflicting views. By pairing positive evaluation with negative evaluation, we identified three pairs, i.e., fear versus maladaptive rewards, descriptive norm versus maladaptive rewards, and subjective norm versus maladaptive rewards, as the antecedents of attitudinal ambivalence. Figure 2a shows the proposed pairs of constructs within PMT that can give rise to attitudinal ambivalence. Figure 2b shows our proposed research model that incorporates attitudinal ambivalence and social norms into PMT. We will develop hypotheses for the new relationships only.

### ***Intrapersonal Process: Fear and Maladaptive Rewards***

According to PMT, individuals will be motivated to engage in protection behaviors only when their fear of cyberattacks outweighs their assessment of maladaptive rewards. When both of them are at roughly the same level, the *oppositional view* will explain the formation of attitudinal ambivalence [53,54]. Specifically, when individuals appraise a fear appeal, they may be scared or worried about the cybersecurity threats mentioned in the fear appeal and think that using security software is a good way to prevent cyberattacks. Meanwhile, they may also perceive not taking protection against cybersecurity threats as rewards gained, such as saving time and effort, and avoiding the disturbance involved in the installation and usage of security software. Under this circumstance, a competing force arises from the



**Figure 2a.** Antecedents of Attitudinal Ambivalence in the Context of Information Security.

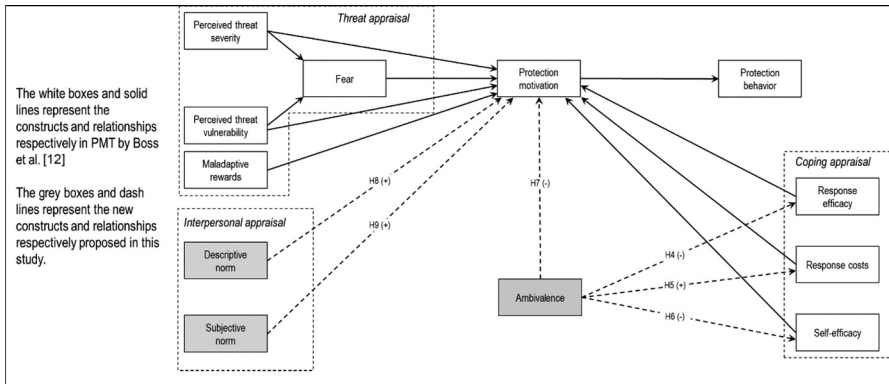


Figure 2b. Proposed Model Incorporating Attitudinal Ambivalence and Social Norms into PMT.

assessment of the detrimental consequences of being a victim of a cyberattack and the benefits of avoiding the hassle and inconvenience in installing and maintaining cybersecurity software. As a result, individuals are likely to experience attitudinal ambivalence. When these competing forces grow stronger, individuals are likely to experience a higher level of attitudinal ambivalence. In line with the *oppositional view*, we argue that when the evaluations of fear and maladaptive rewards are at similar levels, attitudinal ambivalence will increase as the levels of the evaluations increase.

When the levels of fear and maladaptive rewards are at the opposite extremes from each other, i.e., when individuals have a low level of fear but perceive a high level of maladaptive rewards, or vice versa, a *congruent view* will prevail. It is possible that some individuals, e.g., those who are diagnosed with antisocial personality disorder, will experience less or no fear even though the fear appeal is effective because they tend to put themselves in danger or risky situations [36]. Meanwhile, they may perceive a high level of maladaptive rewards resulting from not engaging in protection behaviors that are likely to cost time and effort, or cause disruption to their lives due to the effort required in installing cybersecurity software. Under this circumstance, attitudinal ambivalence is not likely to exist because these individuals will have a clear thought of not taking protection behavior against cybersecurity threats. Along the same line of reasoning, we argue that attitudinal ambivalence is not likely to be observed when individuals have a high level of fear but perceive a low level of maladaptive rewards. Conversely, the degree of congruence will reduce when the level of fear increases or the level of maladaptive rewards decreases in a scenario where perceived fear is low but perceived maladaptive rewards are high. Likewise, in a scenario where perceived fear is high but perceived maladaptive rewards are low, the degree of congruence will reduce when the level of fear decreases or the level of maladaptive rewards increases. The degree of congruence will be at its lowest when the levels of fear and maladaptive rewards are the same. As congruence is the flip side of opposition, attitudinal ambivalence will arise when the degree of congruence decreases. In line with the *congruent view*, we argue that a simultaneous evaluation of fear and maladaptive rewards will have a quadratic effect (inverted U-shape) on attitudinal ambivalence.

We further argue that attitudinal ambivalence will reach its peak when the intensity of conflicting opinions is at its strongest. Our argument is consistent with what was found in prior studies (e.g., [64]). Moody et al.'s [64] study of online consumer behavior found that the degree of attitudinal ambivalence was at its strongest when consumers simultaneously held high levels of trust and distrust in sellers. In the information security context, we argue that in a scenario where individuals hold both high levels of fear and maladaptive rewards, the strongest *oppositional view* will emerge, under which individuals' sense of struggle is at its peak, thus resulting in the highest degree of attitudinal ambivalence as compared to other scenarios, i.e., low fear vs. low maladaptive rewards, high fear vs. low maladaptive rewards, and low fear vs. high maladaptive rewards. Taken together, we hypothesize:

*H1: An individual's simultaneous evaluations of fear and maladaptive rewards will give rise to attitudinal ambivalence. Specifically:*

- (a) *The oppositional view emerging from the evaluations of fear and maladaptive rewards will positively affect attitudinal ambivalence.*
- (b) *The congruent view emerging from the evaluations of fear and maladaptive rewards will have a quadratic effect (inverted U-shape) on attitudinal ambivalence.*
- (c) *The degree of attitudinal ambivalence will reach its peak when individuals have the highest levels of fear and maladaptive rewards.*

### ***Interaction between Intrapersonal and Interpersonal Processes***

In our model, we incorporate an interpersonal appraisal process and argue that attitudinal ambivalence is likely to arise when there is a conflict between intrapersonal and interpersonal appraisal processes. Descriptive norm represents the opinions of the majority whereas subjective norm represents the opinions of the important/significant others, and individuals are more likely to behave in accordance with the majority or the important/significant others as an effective way to deal with novel, ambiguous or uncertain situations [20]. In the information security context, individuals generally do not have much knowledge in cybersecurity and tend to go along with the opinions of the majority or the important/significant others that favor engagement in protection behaviors against cybersecurity threats. However, when individuals perceive a high level of maladaptive rewards, an *oppositional view* to the majority or the important/significant others arises. Specifically, the *oppositional view* can explain the formation of attitudinal ambivalence when maladaptive rewards and descriptive/subjective norm are at similar levels. In both cases, individuals are likely to experience attitudinal ambivalence, and the magnitude of attitudinal ambivalence will increase when the *oppositional view* becomes stronger.

The evaluations of the descriptive/subjective norm and maladaptive rewards will converge when individuals perceive a low level of maladaptive rewards but high descriptive/subjective norm, or vice versa. Under both situations, attitudinal ambivalence is not likely to be observed because individuals have a clear thought of taking/not taking protection behavior. In line with the reasoning for fear and maladaptive rewards, we argue that the degree of congruence will reduce when individuals shift away from the extremes of

maladaptive rewards and descriptive/subjective norm. The degree of congruence will be the lowest when the influence of maladaptive rewards and descriptive/subjective norm are perceived as equally high.

Along the same line of reasoning in H1, we argue that attitudinal ambivalence will reach its peak when the intensity of the *oppositional view* arising from the evaluations of maladaptive rewards and the descriptive/subjective norm is at its strongest. In the information security context, the intensity of such an *oppositional view* is at its strongest when the evaluations of maladaptive rewards and the descriptive/subjective norm are perceived as equally high. Under this circumstance, individuals are likely to experience the highest degree of attitudinal ambivalence. Taken together, we hypothesize:

*H2: An individual's simultaneous evaluations of maladaptive rewards and descriptive norm will give rise to attitudinal ambivalence.*

- (a) *The oppositional view emerging from the evaluations of maladaptive rewards and descriptive norm will positively affect attitudinal ambivalence.*
- (b) *The congruent view emerging from the evaluations of maladaptive rewards and descriptive norm will have a quadratic effect (inverted U-shape) on attitudinal ambivalence.*
- (c) *The degree of attitudinal ambivalence will reach its peak when individuals have the highest levels of maladaptive rewards and descriptive norm.*

*H3: An individual's simultaneous evaluations of maladaptive rewards and subjective norm will give rise to attitudinal ambivalence.*

- (a) *The oppositional view emerging from the evaluations of maladaptive rewards and subjective norm will positively affect attitudinal ambivalence.*
- (b) *The congruent view emerging from the evaluations of maladaptive rewards and subjective norm will have a quadratic effect (inverted U-shape) on attitudinal ambivalence.*
- (c) *The degree of attitudinal ambivalence will reach its peak when individuals have the highest levels of maladaptive rewards and subjective norm.*

### **Attitudinal Ambivalence Outcomes**

We argue that when individuals seek to mitigate attitudinal ambivalence, their perception of efficacy toward the protection behavior is likely to be reshaped based on the domination approach (a defensive mechanism) of the attitudinal ambivalence theory [4] which embraces the biased systematic processing perspective [66]. Such a perception of efficacy corresponds to the coping appraisal process in PMT during which the effectiveness, cost, and ease of engaging in certain protection behavior are assessed. In light of this, we focus on theorizing individuals' coping appraisal processes as a response to the attitudinal ambivalence they experience.

As noted earlier, unbiased systematic processing is cognitively demanding and likely to intensify attitudinal ambivalence, while biased systematic processing requires less cognitive effort as individuals only need to process information that confirms or strengthens their existing beliefs or values. Under the circumstances, individuals are likely to resolve attitudinal ambivalence by adopting a domination approach that nonconsciously amplifies one side of the conflicting thoughts [4]. Specifically, individuals will resort to biased systematic processing where their preheld thoughts or beliefs are reinforced [4,31,48,66]. In the context of information security, individuals are likely to amplify their initial inadequate security awareness toward protection behaviors but ignore information that is not consistent with such beliefs [76]. In line with the literature, we argue that individuals with inadequate cybersecurity awareness and weak motivation to engage in protection behaviors are likely to perceive a low level of response efficacy as they lack confidence in identifying tools or techniques that can help them cope with the cybersecurity threats [38,88]. In brief, attitudinal ambivalence invokes the negative aspects of engaging in protection behavior which stem from individuals' initial inadequate security awareness, making them think that engaging in such behavior against cybersecurity threats is not effective or not useful. In addition, individuals who experience more attitudinal ambivalence are likely to rely more on biased systematic processing, resulting in lower perceived response efficacy.

*H4: Attitudinal ambivalence is negatively related to response efficacy.*

Along the same line of reasoning we provided for H4, individuals who experience attitudinal ambivalence will resort to biased systematic processing that is likely to amplify their initial inadequate security awareness toward the protection behavior. Consequently, the negative aspects of engaging in such behavior will be invoked, incurring a higher level of response cost, such as more effort and time consuming, of engaging in the protection behavior [38]. Due to the lack of security awareness toward the protection behavior, individuals are likely to underestimate the risks of cybersecurity threats while perceiving the security compliance behavior as inconvenient and effortful [16]. Similarly, they are likely to presume that the costs of taking the protection behavior outweigh the benefits [2]. In addition, individuals are likely to use more biased systematic processing when the degree of attitudinal ambivalence increases, resulting in a higher level of perceived response cost.

*H5: Attitudinal ambivalence is positively related to response costs.*

Individuals with weak security awareness will have low levels of beliefs in their capability to perform the security behavior [38], as the negative aspects of engaging in such behavior are invoked due to biased systematic processing [40]. Individuals experiencing attitudinal ambivalence are likely to have a low level of self-efficacy. The self-efficacy theory [6] posits that individuals rely partly on emotional arousal to judge their vulnerability to dysfunction in that they are more likely to have a strong sense of self-efficacy when they are not stressed. However, if they are disturbed by aversive arousal, their self-efficacy beliefs are more likely to diminish. This rationale explains how attitudinal ambivalence affects individuals' self-efficacy beliefs. Specifically, individuals' self-efficacy beliefs are likely to reduce as a

consequence of the stress, discomfort and negative feelings [7] arising from the experience of attitudinal ambivalence. In the context of information security, individuals may experience attitudinal ambivalence if they perceive a high level of fear of cybersecurity threats and a huge amount of effort in using security software, such as those designed for monetary transactions or banking service, especially when they are new users of those software. Such attitudinal ambivalence arouses aversive emotions, which are detrimental to individuals' self-efficacy in coping with the situation.

*H6: Attitudinal ambivalence is negatively related to self-efficacy.*

As noted earlier, attitudinal ambivalence is likely to trigger biased systematic information processing among individuals, leading to more consistency between initially held attitudes/beliefs, which are likely to be negative in our case, and subsequent intentions or motivation to engage in protection behavior. In addition, biased systematic processing will lead to a closer correspondence between attitudes and intentions [53]. In other words, individuals' protection motivation will become more consistent with their attitude when they experience attitudinal ambivalence. Therefore, individuals will resort to their initial inadequate security awareness toward the protection behavior and view the protection behavior more negatively, such as less effective, difficult to use, effortful and time-consuming, when the domination approach is triggered as a mean to relieve the psychological discomfort caused by attitudinal ambivalence [16,38]. Consequently, the inadequate security awareness toward the protection behavior is likely to discourage individuals from adopting such behavior [2]. Overall, individuals' protection motivation is likely reduced when they experience attitudinal ambivalence. This is in line with prior studies that found a negative effect of attitudinal ambivalence on people's pro-environmental behavioral intention [25] and actual behaviors, such as eating meat [11].

*H7: Attitudinal ambivalence is negatively related to protection motivation.*

### **Effects of Social Norms on Protection Motivation**

When individuals believe that most people will engage in protection behavior, their protection motivation is likely to increase because they are afraid of becoming the targets of cybersecurity attacks. Individuals are also likely to value and conform to the views/opinions of important/significant others because they trust and respect those people [13,56,83,92,93]. Prior studies have found positive effects of descriptive norm and subjective norm on individuals' protection motivation [42,86]. Hence, we hypothesize:

*H8: Descriptive norm is positively related to protection motivation.*

*H9: Subjective norm is positively related to protection motivation.*



## METHOD

### *Setting and Procedure*

To test our model, we conducted a study in a public university in Hong Kong to understand what motivates individuals to use 2FA to protect against potential cybersecurity attacks on their email accounts. We chose a university context, as the education sector is one of the most vulnerable to cybersecurity breaches [59]. 2FA is a method of confirming users' identities by using a combination of two different factors, e.g., a password and a verification code sent to a user's phone. Data breach of email accounts is considered detrimental because these accounts could contain sensitive and important personal information [43,74]. A month before our study, the university's IT Services Center disseminated information on 2FA and how it works in their e-newsletters which were sent to all students. We used a field experiment to manipulate fear appeal among the participants. Working with the university's IT Services Center, an email invitation to participate in our study was sent to 8,000 randomly chosen students. The students who clicked a link embedded in the email were directed to our experiment website, where they were weighted-randomly assigned (90% vs. 10% ratio) into either of two conditions: (1) fear appeal (treatment group) and (2) no fear appeal (control group). Given that the main purpose of our study was not to examine the effectiveness of fear appeal, we omitted the low fear condition manipulated in some prior studies (e.g., [12]) but made sure the fear appeal manipulation was properly performed, and set the no fear condition as control. We also assigned more participants to the treatment group in the main study. Participants in the treatment group were directed to a webpage where they first read the threatening message and then the description of 2FA to increase their efficacy of engaging in protection behaviors, whereas those in the control group only read the description of 2FA (Table 3). Next, both groups completed an online questionnaire containing the manipulation checks on fear appeal and the items for various constructs. At the end of the questionnaire, a link was provided for them to register for 2FA if they wished to do so.

### *Measurement and Pilot Study*

Table 4 presents the items used in our study. All PMT constructs were measured using items adapted from the existing literature. For descriptive norm and subjective norm, measures were adapted from Anderson and Agarwal [3]. A single item (the ones with the highest loadings in the pilot study) was used for each of these two variables in the main study, due to the university's IT Services Center's restriction on the questionnaire length. Attitudinal ambivalence was measured using the items adapted from Barden and Petty [8] and Priester and Petty [70] to capture the extent to which participants had conflicted, indecisive or mixed feelings toward using 2FA for email protection. The actual protection behavior, measured as whether the participants adopted 2FA, was coded as 1 if the participants adopted 2FA and 0 otherwise. The adoption data were collected from the university's 2FA computer log. Gender, age, year of study, and program (Undergraduate or Postgraduate) were included as control variables for protection motivation.

A pilot study was conducted among 110 students (50 male), ages between 20 and 24, who enrolled in an undergraduate course at the university. We verified our data collection procedure, the effectiveness of fear manipulation, and the validity of measurement items

**Table 3.** Fear Appeal Manipulation*Without Fear Appeal Condition*

The university is introducing two-factor authentication (2FA) to enhance students' email security. In addition to using a password (i.e., first factor), 2FA verifies your identity with your phone (i.e., second factor) to prevent others from logging into your email account, even if they knew your password.

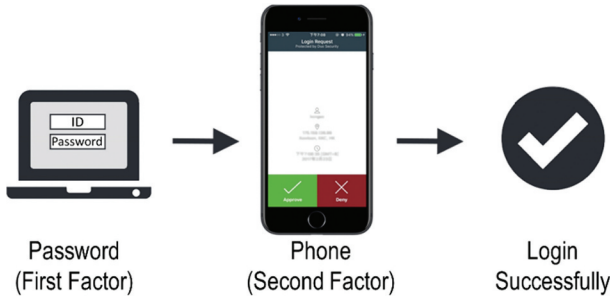


Illustration of 2FA provided to participants

*With Fear Appeal Condition*

According to a recent cybersecurity report, in the past 5 years the number of **unauthorized access to email** accounts has **increased substantially by 25%** due to stolen passwords. You may think email hacking is a very difficult task and you are unlikely to be hacked, but that is not the case as one can easily find many ways to hack an email account by searching on Google. Your email account has **very high risk of being hacked**.

Some ways of email hacking:

- Phishing
- Keystroke capturing
- Password guessing
- Fake wireless access points

Consequences of being hacked:

- Unauthorized release of your personal data (e.g., personal photos, sensitive information)
- Commit crimes using your email
- Spread computer virus and email spam using your email
- Install malware, Trojan, Worm on your computer
- Take control of your computer devices (e.g., webcam, microphone, screen)

The university is introducing two-factor authentication (2FA) to enhance students' email security. In addition to using a password (i.e., first factor), 2FA verifies your identity with your phone (i.e., second factor) to prevent others from logging into your email account, even if they knew your password.

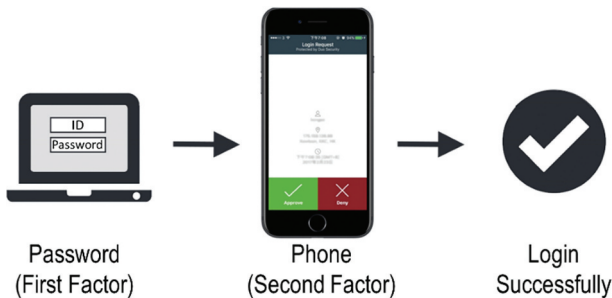


Illustration of 2FA provided to participants

through the pilot study. The procedures went well, supporting our experiment design. We also examined the measurement model and found that the items measuring our constructs demonstrated good reliability, and convergent and discriminant validity. The participants in the pilot study were omitted from the main study.

**Table 4.** Measurement Items

Constructs	Items
Perceived severity [51]	PS1: If my email were hacked, it would affect me severely. PS2: If my email were hacked, it would affect me seriously. PS3: If my email were hacked, it would affect me significantly. PS4: If my email were hacked, it would affect me negatively.
Perceived vulnerability [51]	PV1: My email is vulnerable to be hacked. PV2: It is likely that my email will be hacked. PV3: It is possible that my email will be hacked. PV4: The chance of my email being hacked is high.
Maladaptive rewards [12]	MR1: Not using 2FA for email saves me effort. MR2: Not using 2FA makes it more convenient for me to use email. MR3: Using 2FA would slow down the speed of my access to email. MR4: Using 2FA for email would interfere with my interaction with other apps on my phone. MR5: Using 2FA for email would interfere with my use of other apps on my phone. MR6: Using 2FA for email would interrupt my use of other apps on my phone.
Fear [63]	FE1: I am worried about my email being hacked. FE2: I am frightened about my email being hacked. FE3: I am anxious about my email being hacked. FE4: I am scared about my email being hacked.
Response efficacy [51,63]	RE1: I believe 2FA can help protect my email. RE2: I think 2FA is effective for protecting my email. RE3: I believe 2FA can reduce the risk of my email being hacked. RE4: I think 2FA can lessen the chances of my email being hacked.
Response costs [12]	RC1: Using 2FA for email would require too much work. RC2: Using 2FA for email would require more effort. RC3: Using 2FA for email would be time consuming.
Self-efficacy [93]	SE1: I can use 2FA for email if there was no one around to tell me what to do. SE2: I can use 2FA for email if I could call someone for help if I got stuck. SE3: I can use 2FA for email if I had just the built-in help facility for assistance.
Subjective norm [3]	SN1: People who are important to me think that I should use 2FA for email.
Descriptive norm [3]	DN1: I believe the majority of people adopt 2FA to protect their email from security attacks.
Protection Motivation [51]	PM1: I intend to use 2FA for email in the near future. PM2: I predict I will use 2FA for email in the near future. PM3: I plan to use 2FA for email in the near future.
Attitudinal Ambivalence [8,70]	AM1: To what extent do you feel conflicted in your reactions to using 2FA for email. <sup>1</sup> AM2: To what extent do you feel indecisive in your reactions to using 2FA for email. <sup>2</sup> AM3: To what extent do you feel one-sided or mixed reactions to using 2FA for email. <sup>3</sup>
Fashion Consciousness [62]	FC1: When I must choose between the two, I usually dress for fashion, not for comfort. FC2: An important part of my life and activities is dressing smartly. FC3: A person should try to dress in style.

Notes: All 7-point scales with anchors: "Strongly disagree" = 1 to "Strongly agree" = 7, except for <sup>1</sup> "Not at all" = 1 to "Very conflicted" = 7, <sup>2</sup> "Not at all" = 1 to "Very indecisive" = 7, <sup>3</sup> "One-sided" = 1 to "Mixed" = 7

One concern about the measures of social norms was that students might not have referents for 2FA or do not value their referents' opinions about 2FA, thus threatening the validity of these measures. To alleviate this concern, we conducted a focus group study with two sessions, each comprising of 10 participants (20 participants in total), before the main study to identify who are considered to be the students' referents and whether the referents' opinions about 2FA matter to them. The participants were drawn from the pilot study sample. We found that most participants would generally consider their close peers/friends at school and/or best friends in their life as their referents. They would also consider whether their referents would use 2FA when logging into some online personal services (e.g., online banking) as they were curious whether using 2FA is a common practice.

**Table 5.** Manipulation Checks on Fear Appeals

Conditions	n	Fear	Perceived severity	Perceived vulnerability	Protection motivation
Full sample	1,383	4.40 (1.35) <sup>1</sup>	5.73 (0.93) <sup>1</sup>	4.16 (1.20) <sup>1</sup>	4.74 (1.16) <sup>1</sup>
With fear-appeal subsample (Treatment)	1,232	4.46 (1.33) <sup>1</sup>	5.75 (0.93) <sup>1</sup>	4.26 (1.20) <sup>1</sup>	4.80 (1.13) <sup>1</sup>
Without fear-appeal subsample (Control)	151	4.28 (1.30) <sup>1</sup>	5.55 (1.11) <sup>1</sup>	3.98 (1.18) <sup>1</sup>	4.65 (1.19) <sup>1</sup>
t-test (between groups with and without fear-appeal)		2.12*	2.59*	3.81***	2.05*

Notes: \* $p < .05$ ; \*\*\* $p < .001$ ; <sup>1</sup> Mean (SD).

## RESULTS

In our research context, students are an appropriate population as they are heavy internet users who need to guard against cybersecurity attacks through the use of login access control. As incentives, participants were entered into a lucky draw to win attractive prizes. A total of 1,543 students (out of the randomly selected 8,000) participated in the study. We checked for non-response bias and there was no significant difference in demographics between those who responded to the email and those who did not. We excluded participants who failed to complete the whole questionnaire or answered the checker questions incorrectly, resulting in 1,383 participants (1,232 in the treatment group; 151 in the control group).

Table 5 presents the results of the manipulation checks on fear appeal. Two-sample t-test showed that there were significant mean differences between the treatment and control groups on fear, perceived severity, perceived vulnerability, and protection motivation. The manipulation of fear appeal was effective as there were consistently higher scores for each construct in the treatment group than those in the control group. For the treatment group, the mean age of participants was 21.3 years (SD = 3.1) with 57% male. On average, participants reported they spent 1 to 2 hours reading university emails per day and they had used emails for 6 to 7 years. Among these participants, 26.6% registered for 2FA and there was a significant correlation between protection motivation and adoption behavior ( $r = 0.18$ ;  $p < .01$ ;  $n = 1,232$ ). For the control group, we found that no students registered for 2FA. Based on these results, we believe that individuals exposed to the fear appeal (treatment group) were more likely to engage in the protection behavior than those not exposed to the fear appeal (control group), which is in line with the existing information security literature. Subsequent data analysis was based on the treatment group. Following prior literature on PMT (e.g., [12]), we excluded the control group data from subsequent analysis when the fear-appeal manipulation was found to be ineffective.

### Measurement Model Testing

Table 6 shows the descriptive statistics and correlations of our scales. Attitudinal ambivalence, descriptive norm, subjective norm, and all PMT constructs were significantly correlated with protection motivation in the expected directions. In addition, descriptive norm and subjective norm were significantly correlated with attitudinal ambivalence. We checked for construct reliability, convergent validity, and discriminant validity using AMOS version



**Table 6.** Descriptive Statistics and Correlations (Fear Appeal Group)

	Mean	SD	CR	AVE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1 Age	21.31	3.10	-	-	-															
2 Gender	1.43	0.49	-	-	-	-0.13**														
3 Program	1.48	1.02	-	-	0.72**	-0.13**														
4 Year of study	2.37	1.16	-	-	0.30**	-0.02	-0.05													
5 Fear	4.46	1.33	.94	.90	0.02	0.13**	0.02	0.03	0.95											
6 Perceived threat severity	5.75	0.93	.93	.90	0.09**	-0.06*	0.11**	-0.00	0.36**	0.95										
7 Perceived threat vulnerability	4.26	1.20	.86	.77	0.06**	0.14**	0.05	0.04	0.56**	0.23**	0.88									
8 Maladaptive rewards	3.62	1.33	.87	.78	0.04	0.01	0.03	0.04	0.06*	-0.04	0.05	0.88								
9 Response efficacy	5.38	0.91	.95	.91	0.05*	-0.09**	0.02	0.03	0.20**	0.24**	0.17**	-0.23**	0.95							
10 Response costs	3.89	1.17	.87	.71	0.01	-0.04	-0.02	0.02	-0.07*	-0.08*	-0.04	-0.58**	-0.15**	0.84						
11 Self-efficacy	5.08	1.01	.87	.83	0.03	-0.03	0.03	0.03	0.15**	0.23**	0.12**	-0.36**	0.60**	-0.30**	0.91					
12 Attitudinal ambivalence	3.06	0.79	.81	.60	-0.03	0.01	-0.06*	0.03	-0.02	-0.12**	-0.03	0.49**	-0.26**	-0.59**	-0.43**	0.77				
13 Descriptive norm	4.79	1.38	-	-	-0.06*	0.04	-0.05	-0.03	0.17**	0.13**	0.12**	-0.18**	0.34**	-0.22**	0.39**	-0.26**	-			
14 Subjective norm	4.21	1.11	-	-	-0.02	0.04	-0.02	-0.05	0.25**	0.13**	0.19**	-0.12**	0.28**	-0.19**	0.33**	-0.20**	0.35**	-		
15 Protection motivation	4.80	1.13	.96	.95	-0.01	0.03	-0.00	-0.03	0.30**	0.23**	0.26**	-0.41**	0.47**	-0.52**	0.61**	-0.49**	0.48**	0.43**	0.97	

Notes:  $n = 1,232$ ;  $*p < .05$ ;  $**p < .01$ ;  $***p < .001$ ; CR = Composite Reliability; The diagonal indicates the square root of AVE.

26. Model fit was acceptable ( $\chi^2/df = 4.81$ ; CFI = 0.954; TLI = 0.946; RMSEA = 0.038) [49]. Reliability was supported as the composite reliabilities (CRs) were greater than 0.70 [34]. Convergent validity was supported as the item loadings and the AVEs were greater than .70 and .50 respectively. Discriminant validity was also established as the square roots of the AVE for our constructs were greater than the correlations between constructs [34]. We also assessed discriminant validity by comparing model fits between our measurement model and other competing models [12]. The results are reported in Appendix C. In all cases, our measurement model was significantly better than the competing models, thus demonstrating discriminant validity. All variance inflation factors (VIFs) were below 4, indicating that multicollinearity between constructs was not a concern.

**Polynomial Regression with Response Surface Analysis**

H1 to H3 do not simply hypothesize the interaction effects that can only capture the overall dependency between two constructs without disentangling it into the *oppositional view* (when the levels of positive and negative evaluations are similar) and *congruent view* (when the levels of positive and negative evaluations are opposite to each other). Instead, these nuanced differences can be better captured using polynomial regression with surface response analysis due to its ability to model nonlinear relationship, identify complex effect patterns, and help better visualize the simultaneous change in positive and negative evaluations [10,32,55]. Specifically, by employing polynomial regression with surface

**Table 7.** Polynomial Regression Analysis of Attitudinal Ambivalence (Fear-Appeal Group)

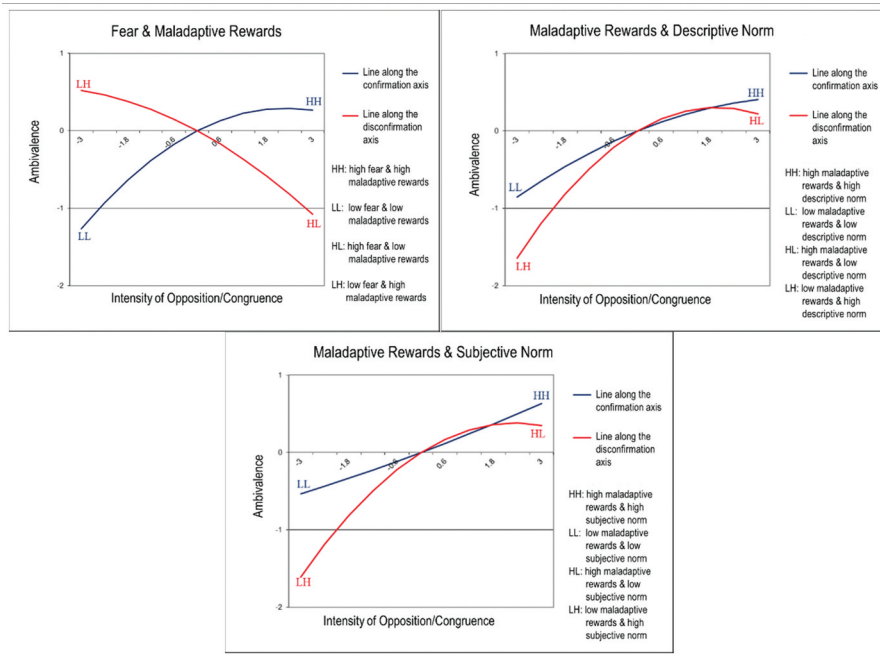
	1st-Order Linear Model	2nd-Order Quadratic Model
R <sup>2</sup>	.29	.32
ΔR <sup>2</sup>	.29***	.03***
<i>First-Order Terms</i>		
Fear	.00	-.01
Maladaptive rewards	.32***	.26***
Descriptive norm	-.10***	-.05**
Subjective norm	-.08***	-.07**
<i>Second-Order Terms</i>		
Fear × Fear		-.01
Maladaptive rewards × Maladaptive rewards		-.04**
Descriptive norm × Descriptive norm		-.02
Subjective norm × Subjective norm		.01
Fear × Maladaptive rewards		-.01
Maladaptive rewards × Descriptive norm		.03*
Maladaptive rewards × Subjective norm		.04*

Notes: n = 1,232; \*p < .05; \*\*p < .01; \*\*\*p < .001

**Table 8.** Response Surface Analysis of Attitudinal Ambivalence (Fear-Appeal Group)

	Linear Slope	Quadratic Slope
<i>Along the Confirmation Axis</i>		
Fear × Maladaptive rewards	.25***	-.06**
Maladaptive rewards × Descriptive norm	.21***	-.03
Maladaptive rewards × Subjective norm	.19***	.01
<i>Along the Disconfirmation Axis</i>		
Fear × Maladaptive rewards	-.27***	-.03
Maladaptive rewards × Descriptive norm	.31***	-.08***
Maladaptive rewards × Subjective norm	.33***	-.07**

Notes: n = 1,232; \*p < .05; \*\*p < .01; \*\*\*p < .001



**Figure 3.** Plots of Lines along the Confirmation and Disconfirmation Axes

response analysis, we were able to provide a holistic view on the formation of attitudinal ambivalence through an examination of the slopes along the confirmation and disconfirmation axes, which correspond to the *oppositional view* and the *congruent view* respectively. To test H1 to H3, we examined the linear slopes along the confirmation axes (H1a, H2a, and H3a) and the quadratic slopes along the disconfirmation axes (H1b, H2b, and H3b). In addition, we looked at the response surfaces to examine whether the highest levels of positive and negative evaluations correspond to the highest levels of attitudinal ambivalence (H1c, H2c, and H3c). Appendix D provides a brief description of this statistical technique.

Table 7 shows the results of the polynomial regression analysis. Table 8 reports the linear and quadratic slopes for the proposed pairs of constructs. Figure 3 shows the plots along both the confirmation and disconfirmation axes for each pair of constructs. We also provide the response surface diagrams for H1-H3 in Appendix E. H1 hypothesizes attitudinal ambivalence will arise from the intrapersonal process (i.e., threat appraisal process). From Table 8, along the confirmation axis, the linear slope of the paired constructs, i.e., fear and maladaptive rewards, was positive and significant ( $\beta = .25, p < .001$ ), thus supporting H1a. However, along the disconfirmation axis, the quadratic slope ( $\beta = -.03, p > .05$ ) was not significant. Thus, H1b was not supported. H1c was also not supported, as Figure 3 shows that the point corresponding to HH was not the highest. In summary, H1 was partially supported.

H2 and H3 hypothesize attitudinal ambivalence will arise from an interaction between the intrapersonal and interpersonal processes, i.e., threat appraisal process and descriptive norm (H2) and subjective norm (H3). From Table 8, along the confirmation axis, the linear slopes of the two pairs of constructs, i.e., maladaptive rewards and descriptive norm

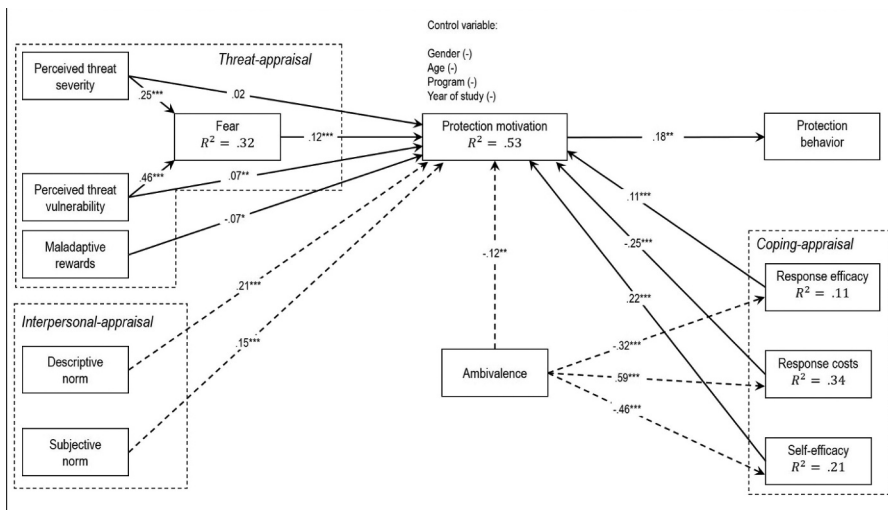


( $\beta = .21, p < .001$ ), and maladaptive rewards and subjective norm ( $\beta = .19, p < .001$ ) were both positive and significant, thus supporting H2a and H3a. Along the disconfirmation axis, the quadratic slopes of both paired constructs, i.e., maladaptive rewards and descriptive norm ( $\beta = -.08, p < .001$ ), and maladaptive rewards and subjective norm ( $\beta = -.07, p < .01$ ) were also significant, thus supporting H2b and H3b. The plot for maladaptive rewards and subjective norm clearly shows that the point corresponding to *HH* was the highest, which was also the case for maladaptive rewards and descriptive norm. Therefore, both H2c and H3c were supported. In summary, both H2 and H3 were fully supported.

**Table 9.** Model Results for Protection Motivation (Fear-Appeal Group)

	Model 1	Model 2	Model 3
R <sup>2</sup>	.00	.50	.53
ΔR <sup>2</sup>	.00	.49***	.03***
<i>Control Variables</i>			
Age	.02	.02	.02
Gender	.03	.00	-.01
Program	-.04	-.06	-.05
Year of study	-.04	-.05	-.04
<i>PMT Variables</i>			
Fear		.16***	.12***
Maladaptive rewards		-.08**	-.07*
Perceived threat severity		.02	.02
Perceived threat vulnerability		.07**	.07**
Response efficacy		.14***	.11***
Response costs		-.31***	-.25***
Self-efficacy		.34***	.22***
<i>New Variables</i>			
Descriptive norm			.21***
Subjective norm			.15***
Attitudinal ambivalence			-.12**

Notes:  $n = 1,232$ ; \* $p < .05$ ; \*\* $p < .01$ ; \*\*\* $p < .001$



**Figure 4.** Model Results for Fear-Appeal Group

A plausible explanation for why H1 was partially supported is that maladaptive rewards are likely to be a more dominant driver of attitudinal ambivalence than fear in the context of information security because we found that attitudinal ambivalence was high (low) when maladaptive rewards were high (low), regardless of the evaluation of fear (Figure 3). Furthermore, H2 and H3 were fully supported, indicating that attitudinal ambivalence is likely to arise when individuals simultaneously evaluate the benefits of not engaging in protection behaviors and the opinions of the majority and important others.

### Structural Model Testing

We tested H4 to H9 with AMOS version 26 using the sample of the treatment group ( $n = 1,232$ ). The model fit indices were acceptable ( $\chi^2/df = 5.02$ ; CFI = 0.931; TLI = 0.919; RMSEA = 0.057) [49] and our model explained 53% of variance in protection motivation (see Model 3 of Table 9). We also checked the model based on the control group ( $n = 151$ ) and the results showed that, consistent with prior studies (e.g., [12]), certain relationships specified in the original PMT model were not supported (see Appendix F). These findings suggest that our fear appeal was manipulated properly and effectively in arousing fear among the participants. Figure 4 show that the effects of attitudinal ambivalence on response efficacy ( $\beta = -.32, p < .001$ ) and self-efficacy ( $\beta = -.46, p < .001$ ) were negative and significant, whereas on response costs ( $\beta = .59, p < .001$ ) was positive and significant, thus supporting H4, H5, and H6. H7 was supported as attitudinal ambivalence was significantly and negatively related to protection motivation ( $\beta = -.12, p < .01$ ). Finally, the effects of descriptive norm ( $\beta = .21, p < .001$ ) and subjective norm ( $\beta = .15, p < .001$ ) on protection motivation were both positive and significant, thus supporting H8 and H9. Table 10 summarizes the results of hypotheses testing.

Given that our data were collected from students through a questionnaire, we assessed the influence of common method bias using three tests: (1) Harman single factor, (2) common latent factor, and (3) correlational marker technique [58,69,71]. Using Harman's single factor test, we found that the common factor explained only 23.75% of the total variance, well below the commonly accepted threshold of 50%. For the common latent factor analysis, the factor loadings remained stable across the original measurement model when a common method variance factor was included. For the correlational marker technique, we chose fashion consciousness as the marker variable. The smallest observed

**Table 10.** Results of Hypotheses Testing

Hypotheses	Results
H1: Fear vs. Maladaptive rewards $\rightarrow$ Attitudinal ambivalence	Partially supported
H2: Maladaptive rewards vs. Descriptive norm $\rightarrow$ Attitudinal ambivalence	Supported
H3: Maladaptive rewards vs. Subjective norm $\rightarrow$ Attitudinal ambivalence	Supported
H4: Attitudinal Ambivalence is negatively related to response efficacy	Supported
H5: Attitudinal Ambivalence is positively related to response costs	Supported
H6: Attitudinal Ambivalence is negatively related to self-efficacy	Supported
H7: Attitudinal Ambivalence is negatively related to protection motivation	Supported
H8: Descriptive norm is positively related to protection motivation	Supported
H9: Subjective norm is positively related to protection motivation	Supported

positive correlation between the marker variable and other variables was 0.023. All corrected zero-order correlations remained statistically significant after controlling for common method variance, suggesting that common method bias was not a concern.

### **Robustness Checks**

There was a potential issue concerning the effectiveness of fear manipulation, given the small mean difference in fear between the treatment and control groups, i.e., 0.18 with a Cohen's  $d$  of 0.14 [22]. To address this concern, we conducted robustness checks by comparing different subsamples (with different mean scores of fear) in the treatment group with the control group. Specifically, we identified four subsamples from the treatment group corresponding to participants whose mean fear scores were (1) greater than 0.5 SD below the original mean of 4.46 (Cohen's  $d = 0.35$ ), (2) greater than 0.25 SD below the original mean of 4.46 (Cohen's  $d = 0.58$ ), (3) greater than the original mean of 4.46 (Cohen's  $d = 0.75$ ), and (4) greater than 0.25 SD above the original mean of 4.46 (Cohen's  $d = 0.93$ ), respectively. A graphical illustration of this subsampling approach (Figure G1 of Appendix G) and the manipulation checks are provided (see Tables G3, G6, G9, G12 of Appendix G). The results showed that the means of fear in these four subgroups were all significantly higher than those in the control group. We then conducted model testing using these subsamples, and all the results of model testing were consistent with the main study (see Table G2 of Appendix G). Tables G3 to G14 of Appendix G provide more details on the results of model testing.

Another potential issue was the use of single-item measures for descriptive norm and subjective norm, raising concern about the reliability of these two scales. To address this concern, we conducted robustness checks of our structural model [67]. Specifically, we assumed a non-zero measurement error variance and a lower than one reliability score for the single-item latent variables (i.e., descriptive norm and subjective norm) in fitting the model, and set the measurement error variance equaled to the sample variance of the item multiplied by one minus the scale reliability estimate [67]. The scale reliability estimate can be a conservative and arbitrary value of 0.85, or chosen from other studies using similar measure [61]. In this study, the estimated sample variance of descriptive norm and subjective norm were 1.89 and 1.22, respectively. We then performed a sensitivity analysis using four different values of reliability estimate (i.e., 0.9, 0.8, 0.7, and 0.6). All the results across different values of reliability estimate were consistent with the main study, thus alleviating the concern about the single-item measures for descriptive norm and subjective norm.

## **DISCUSSION**

This study aims to shed light on the inconsistent findings across previous PMT-related studies. Drawing on the attitudinal ambivalence theory, we incorporate attitudinal ambivalence into PMT and examine its relationships with the existing variables in PMT. Using polynomial regression with surface response methodology, we avoid the limitations of linear regression models and gain a more holistic and nuanced understanding of the effects of PMT antecedents on attitudinal ambivalence. We theorize why and how attitudinal ambivalence emerges from the intrapersonal and interpersonal appraisal processes, and why and how it influences protection motivation and the coping appraisal process. We

found that attitudinal ambivalence is created when individuals' evaluation of maladaptive rewards is at odds with their evaluations of descriptive norm and subjective norm. Further, attitudinal ambivalence formed in the fear appraisal process has a significant direct impact on protection motivation and the coping appraisal process.

### **Theoretical Contributions**

This study offers several theoretical contributions to the information security literature in general (e.g., [1,44,90]) and more specifically to the literature on PMT (e.g., [27,65]). First, we have extended the literature on information security by providing a new and alternative explanation for how PMT operates through the lens of attitudinal ambivalence to gain a better understanding of individuals' protection motivation against cybersecurity threats. Although prior information security research on PMT (e.g., [12,65]) has identified various personal and social factors that may affect individuals' protection motivation, there are inconsistent findings across these studies. Our study has theorized and empirically validated that the inconsistent findings may be due to an omitted variable, i.e., attitudinal ambivalence. Specifically, attitudinal ambivalence mediates the effects of threat and interpersonal appraisal processes on protection motivation, and the mediation effects emerge only when the evaluations of threat and interpersonal appraisal processes are at odds. Given that attitudinal ambivalence negatively affects protection motivation, such negative effects, if not teased out, are likely to cause the total effects of threat and interpersonal appraisal processes on protection motivation to be close to zero [96], resulting in insignificant relationships between threat/interpersonal appraisal processes and protection motivation. In addition, attitudinal ambivalence may suppress the effects of coping appraisal processes on protection motivation, resulting in insignificant relationships between coping appraisal processes and protection motivation, especially when the correlations between attitudinal ambivalence and protection motivation, and/or the correlations between attitudinal ambivalence and the coping appraisal process are high. Under this circumstance, the inconsistent findings in prior PMT studies may be reconciled by incorporating attitudinal ambivalence into PMT. Thus, the attitudinal ambivalence lens offers a more holistic and nuanced view of the nomological network of PMT by systematically integrating the intrapersonal and interpersonal processes as well as offering a new link between the threat and coping processes through attitudinal ambivalence, which is largely neglected in previous research, to understand individuals' protection motivation against cybersecurity threats.

Second, we identify the interdependent antecedents of attitudinal ambivalence in the information security context. We show that attitudinal ambivalence emerges when individuals simultaneously examine the intrapersonal and interpersonal appraisal processes. In particular, our work shows that maladaptive rewards from the intrapersonal process and social norms (i.e., both descriptive norm and subjective norm) from the interpersonal process represent the key sources of attitudinal ambivalence in the information security context. This missing piece of the puzzle advances our understanding of the role of fear appeal by providing a more holistic view of how the effects of intrapersonal and interpersonal appraisal processes are interdependent.

Third, our study is among the first to explain individuals' coping appraisal and protection motivation using the attitudinal ambivalence theory. The extant PMT studies in information security suggest that fear appeal can emphasize the coping behavior to increase individuals' efficacy in taking the protection precaution [65,77]. Our work indicates that individuals' attitudinal ambivalence toward security behavior has a significant impact on protection motivation as well as the coping appraisal process. This finding is noteworthy as it suggests an alternative path for the fear appeal to influence individuals' coping appraisal process.

Finally, our study contributes to the attitudinal ambivalence theory in general by identifying and theorizing the context-specific antecedents and consequences of attitudinal ambivalence in the information security setting [46]. Specifically, we identified maladaptive rewards as an important source of attitudinal ambivalence in the information security context and paired it with constructs representing the positive evaluation toward protection behaviors against cybersecurity threats. We draw from the *oppositional* and *congruent views* to explain how these pairs can give rise to attitudinal ambivalence. This conceptualization of antecedents that pairs different levels of positive and negative evaluations toward an attitude object goes beyond the traditional approaches, which only consider the individual or interaction effects of these antecedents, and suggests a new avenue for future research. We also elaborate on the consequences of attitudinal ambivalence by theorizing its impact on the coping appraisal process and protection motivation. Such theorization helps explain how and why individuals' protection motivation changes when they experience attitudinal ambivalence toward security behavior. It also provides insights into the design of effective fear appeal that persuades individuals to take protective actions.

### **Practical Implications**

This research also offers practical implications. First, our study suggests that a key factor, i. e., attitudinal ambivalence, can reduce individuals' protection motivation. Attitudinal ambivalence is triggered by the threat/fear appeal which is meant to scare individuals and persuade them to follow the recommended action. Organizations should be made aware of the negative consequences due to attitudinal ambivalence, such as that resulting from a security warning message which triggers an equal amount of fear and maladaptive rewards. Organizations need to design and deploy the fear appeal mindfully to reduce the possibility of triggering ambivalence. In brief, more time and effort should be put into designing an appropriate and effective fear appeal that not only delivers the intended persuasive message to their employees but also reduces their ambivalent feelings toward taking protection behavior.

Second, our findings indicate that the invoked attitudinal ambivalence can significantly affect individuals' coping appraisal process. Ambivalent individuals will perceive security behavior as less effective and more time and effort consuming, which can potentially undermine the efficacy of the fear appeal. Our findings thus inform organizations of the main rationale behind the ineffectualness of a fear appeal and prompt them to analyze the situation for viable solutions. Specifically, organizations should formulate a strategy to avoid invoking ambivalent attitudes among their employees when they process a fear appeal. One

potential solution is to constantly collect feedback from employees via surveys or short meetings, and use the feedback to design more effective fear appeals. Another solution is to incorporate attitude ambivalence into the design of gamified security training systems [78].

Third, understanding the sources of attitudinal ambivalence in the information security context can help companies gain better control of it. Our study has identified important antecedents of attitudinal ambivalence, i.e., maladaptive rewards and social norms. Companies can leverage these findings by deploying an effective security system that minimizes users' time and effort in using the system (e.g., [44,90]) to reduce the negative impact of maladaptive rewards on protection motivation. For example, a better designed 2FA can allow users to save the parameters for login in specific devices, e.g., personal smartphones, such that individuals do not need to verify their identities every time they use their personal devices for login. Furthermore, prior to the implementation of cybersecurity controls to protect the information systems, organizations may conduct an in-depth investigation to assess employees' perceived maladaptive rewards with regard to embracing various security measures. These investigations can help organizations to gain a better understanding of how to design an effective fear appeal.

Finally, companies can consider leveraging the influence of social norms by establishing an organizational culture that motivates the use of protection behavior among individuals. One potential strategy is to promote relevant cybersecurity knowledge and security system to the most influential people (e.g., senior managers or employees who occupy central positions in their social networks) in the company. Once the influential people are convinced to engage in protection behaviors, they can help develop a norm whereby others to whom they connect or interact with in the company are more likely to follow their behaviors.

### **Limitations and Future Research**

There are some limitations in our study. First, we tested our hypotheses with data from only one organization. Future research can cross-validate our model in other settings, including other companies, technology, and countries, to confirm the generalizability of our findings. Second, we used single-item measures for descriptive norm and subjective norm to shorten the length of the questionnaire due to a restriction imposed by our research site. Future research can use multiple-items for these constructs to confirm our findings. Third, we examined the effect of attitudinal ambivalence within the core nomological network of PMT in this study. Future research can examine other factors, e.g., personality traits, disposition, culture, that could potentially give rise to attitudinal ambivalence in the information security context.

### **CONCLUSION**

Cybersecurity is an important issue for both individuals and organizations. Under the circumstances, cybersecurity relies heavily on individuals' awareness of cybersecurity threats and their motivation to engage in protection behaviors. Given that individuals are the weakest link in the cybersecurity chain [30], organizations should uncover and better manage the sources that are likely to discourage their employees and customers from engaging in protection behaviors. Our study contributes to this effort by clarifying the

inconsistent findings in PMT studies and identifying the central role of attitudinal ambivalence in explaining the mechanisms from PMT antecedents to PMT outcomes. Finally, our study contributes to cybersecurity practices in designing and deployment of effective fear appeals.

## Acknowledgements

The authors thank the associate editor, reviewers, and Editor-in-Chief for their constructive comments on earlier versions of this paper.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

This project was partially funded by the Theme-based Research Grant on Fintech (T31-608/18N) of the Research Grant Council of Hong Kong.

## Notes on contributors

**Ka Chung Ng** (borisnkc@gmail.com) is an Assistant Professor in the Department of Management and Marketing, Faculty of Business, Hong Kong Polytechnic University. He received his Ph.D. in Information Systems from the Hong Kong University of Science and Technology. His research interests are in fake news, business analytics, and fintech. His work has appeared in the *Journal of Management Information Systems* and *ACM Transactions on Management Information Systems*.

**Xiaojun Zhang** (xiaojunzhang@ust.hk) is an Associate Professor of Information Systems in the School of Business and Management at the Hong Kong University of Science and Technology. He received his Ph.D. from the University of Arkansas. His primary research stream focuses on understanding the impacts of technology on performance outcomes. Dr. Zhang's research has been published in various journals, including *Information Systems Research*, *Journal of Management Information Systems*, *MIS Quarterly*, *Journal of the Association for Information Systems*, and *European Journal of Information Systems*. He is an Associate Editor of *MIS Quarterly*.

**James Y. L. Thong** (jthong@ust.hk; **corresponding author**) is the Michael Jebsen Professor of Business and Chair Professor of Information Systems in the School of Business and Management, Hong Kong University of Science and Technology. He received his Ph.D. from the National University of Singapore. His research on technology adoption, e-government, human-computer interaction, information privacy, and software piracy has 27,000+ Google Scholar citations and 12,500+ SCOPUS citations. He received the *ISR* Best Associate Editor Award, and is a Senior Editor of *MIS Quarterly* and an AIS Fellow.

**Kar Yan Tam** (kytam@ust.hk) is Dean of the Business School and Chair Professor of Information Systems, Business Statistics and Operations Management at the Hong Kong University of Science and Technology (HKUST). He received his Ph.D. in Management Information Systems from Purdue University. He joined HKUST in 1992 as a founding member of the Business School. Dr. Tam is a Board Member of EFMD and AACSB. His research interests lie in data analytics, fintech, and diffusion of innovations in organizations. He has published in *Journal of Management Information Systems*, *MIS Quarterly*, *Information Systems Research*, *Management Science*, and other journals and serves on the editorial board of a number of IS journals.



## ORCID

Ka Chung Ng  <http://orcid.org/0000-0001-7875-8194>  
 Xiaojun Zhang  <http://orcid.org/0000-0003-0276-3290>  
 James Y. L. Thong  <http://orcid.org/0000-0002-1640-0581>  
 Kar Yan Tam  <http://orcid.org/0000-0003-3242-0184>

## REFERENCES

1. Aloysius, J.A.; Hoehle, H.; Goodarzi, S.; and Venkatesh, V. Big data initiatives in retail environments: Linking service process perceptions to shopping outcomes. *Annals of Operations Research*, 270, 1 (2018), 25–51.
2. Alsaleh, M.; Alomar, N., and Alarifi, A. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*, 12, 3 (2017), e0173284.
3. Anderson, C.L., and Agarwal, R. Practicing safe computing: An multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, 3 (2010), 613–643.
4. Ashforth, B.E.; Rogers, K.M.; Pratt, M.G.; and Pradies, C. Ambivalence in organizations: A multilevel approach. *Organization Science*, 25, 5 (2014), 1453–1478.
5. Aurigemma, S., and Mattson, T. Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems*, 20, 12, (2019), 1700–1742.
6. Bandura, A. Self-Efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84, 2 (1977), 191–215.
7. Bandura, A., and Adams, N. Analysis of self-efficacy theory of behaviour change. *Cognitive Therapy and Research*, 1, 4 (1977), 287–310.
8. Barden, J., and Petty, R.E. The mere perception of elaboration creates attitude certainty: Exploring the thoughtfulness heuristic. *Journal of Personality and Social Psychology*, 95, 3 (2008), 489–509.
9. Benjamin, V.; Zhang, B.; Nunamaker, J.F.J.; and Chen, H. Examining hacker participation length in cybercriminal internet-relay-chat communities. *Journal of Management Information Systems*, 33, 2 (2016), 482–510.
10. Benlian, A. Effect mechanisms of perceptual congruence between information systems professionals and users on satisfaction with service. *Journal of Management Information Systems*, 29, 4 (2013), 63–96.
11. Berndsen, M., and van der Pligt, J. Ambivalence towards meat. *Appetite*, 42, 1 (2004), 71–78.
12. Boss, S.R.; Galletta, D.F.; Lowry, P.B.; Moody, G.D.; and Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39, 4 (2015), 837–864.
13. Brown, S.A.; Dennis, A.R.; and Venkatesh, V. Predicting collaboration technology use: Integrating technology adoption and collaboration research. *Journal of Management Information Systems*, 27, 2 (2010), 9–53.
14. Brown, S.A.; Venkatesh, V.; and Goyal, S. Expectation confirmation in technology use. *Information Systems Research*, 23, 2 (2012), 474–487.
15. Brown, S.A.; Venkatesh, V.; and Goyal, S. Expectation confirmation in information systems research: A test of six competing models. *MIS Quarterly*, 38, 3 (2014), 729–756.
16. Bulgurcu, B.; Cavusoglu, H.; and Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34, 3 (2010), 523–548.
17. Cenfetelli, R.T. Inhibitors and enablers as dual factor concepts in technology usage. *Journal of the Association for Information Systems*, 5, 11–12 (2004), 472–492.
18. Cenfetelli, R.T., and Schwarz, A. Identifying and testing the inhibitors of technology usage intentions. *Information Systems Research*, 22, 4 (2011), 808–823.

19. Chen, Y., and Zahedi, F.M. Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, 40, 1 (2016), 205–222.
20. Cialdini, R.B., and Trost, M.R. Social influence: Social norms, conformity and compliance. In D. Gilbert, S. Fiske and G. Lindzey, (eds.), *The Handbook of Social Psychology*. New York: McGraw-Hill, 1998, pp. 151–192.
21. Cisco. Cisco 2018 annual cybersecurity report. 2018. [https://www.cisco.com/c/dam/m/hu\\_hu/campaigns/security-hub/pdf/acr-2018.pdf](https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf).
22. Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*. Lawrence Erlbaum Associates, 1988.
23. Conner, M., and Armitage, C.J. Attitudinal ambivalence. In W.D. Crano and R. Prislin, (eds.), *Attitudes and Attitude Change*. New York: Psychology Press, 2008, pp. 261–288.
24. Conner, M., and Sparks, P. Ambivalence and attitudes. *European Review of Social Psychology*, 12, 1 (2002), 37–70.
25. Costarelli, S., and Colloca, P. The effects of attitudinal ambivalence on pro-environmental behavioral intentions. *Journal of Environmental Psychology*, 24, 3, 279–288.
26. Cramer, P. Coping and defense mechanisms: What's the difference? *Journal of Personality*, 66, 6 (1998), 919–946.
27. Crossler, R.E., and Bélanger, F. An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *SIGMIS Database*, 45, 4 (2014), 51–71.
28. Crossler, R.E.; Long, J.H.; Loraas, T.M.; and Trinkle, B.S. Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, 28, 1 (2014), 209–226.
29. Dang-Pham, D., and Pittayachawan, S. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, 48, (2015), 281–297.
30. Densham, B. Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, 2015, 1 (2015), 5–8.
31. Ditto, P.H., and Lopez, D.F. Motivated skepticism: Use of differential decision criteria for preferred and nonpreferred conclusions. *Journal of Personality and Social Psychology*, 63, 4 (1992), 568–584.
32. Edwards, J.R. Alternatives to difference scores: Polynomial regression analysis and response surface methodology. In F. Drasgow and N. Schmidt, (eds.), *Measuring and Analyzing Behavior in Organizations: Advances in Measurement and Data Analysis*. San Francisco, US: Jossey-Bass, 2002, pp. 350–400.
33. Festinger, L. *A Theory of Cognitive Dissonance*. Stanford University Press, 1957.
34. Fornell, C., and Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18, 1 (1981), 39–50.
35. Goode, S.; Hoehle, H.; Venkatesh, V.; and Brown, S.A. User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, 41, 3 (2017), 703–727.
36. Goodwin, D., and Guze, S.B. Sociopathy (antisocial personality). In D. Goodwin and S.B. Guze, (eds.), *Psychiatric Diagnosis*. New York, US: Oxford University Press, 1989, pp. 209–225.
37. Gunson, N.; Marshall, D.; Morton, H.; and Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30, 4 (2011), 208–220.
38. Hanus, B., and Wu, Y.A. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33, 1 (2016), 2–16.
39. van Harreveld, F.; van der Pligt, J., and Liver, D. The agony of ambivalence and ways to resolve it: Introducing the MAID model. *Personality and Social Psychology Review*, 13, 1 (2009), 45–61.

40. van Harreveld, F.; Rutjens, B.T.; Rotteveel, M.; Nordgren, L.F., and van der Pligt, J. Ambivalence and decisional conflict as a cause of psychological discomfort: Feeling tense before jumping off the fence. *Journal of Experimental Social Psychology*, 45, 1 (2009), 167–173.
41. Heider, F. Attitudes and cognitive organization. *The Journal of Psychology*, 21, (1946), 107–112.
42. Herath, T., and Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18, 2 (2009), 106–125.
43. Higgins, K.J. Millions of stolen US university email credentials for sale on the dark web. *Dark Reading*, 2017. <https://www.darkreading.com/threat-intelligence/millions-of-stolen-us-university-email-credentials-for-sale-on-the-dark-web-/d/d-id/1328511> .
44. Hoehle, H.; Aloysius, J.A.; Goodarzi, S.; and Venkatesh, V. A nomological network of customers' privacy perceptions: Linking artifact design to shopping efficiency. *European Journal of Information Systems*, 28, 1 (2019), 91–113.
45. Hong, W.; Chan, F.K.Y.; and Thong, J.Y.L. Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, 168, 3 (2021), 539–564.
46. Hong, W.; Chan, F.K.Y.; Thong, J.Y.L.; Chasalow, L.; and Dhillon, G. A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, 25, 1 (2014), 111–136.
47. Hong, W., and Thong, J.Y.L. Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 37, 1 (2013), 275–298.
48. de Hoog, N.; Stroebe, W.; and de Wit, J.B.F. The processing of fear-arousing communications: How biased processing leads to persuasion. *Social Influence*, 3, 2 (2008), 84–113.
49. Hu, L., and Bentler, P.M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6, 1 (1999), 1–55.
50. Jansen, J.; Veenstra, S.; Zuurveen, R.; and Stol, W. Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology*, 35, 5 (2016), 368–379.
51. Johnston, A.C., and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34, 1 (2010), 549–566.
52. Johnston, A.C.; Warkentin, M.; and Siponen, M. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39, 1 (2015), 113–134.
53. Jonas, K.; Diehl, M., and Bromer, P. Effects of attitudinal ambivalence on information processing and attitude-intention consistency. *Journal of Experimental Social Psychology*, 33, 2 (1997), 190–210.
54. Kaplan, K.J. On the ambivalence-indifference problem in attitude theory and measurement: A suggested modification of the semantic differential technique. *Psychological Bulletin*, 77, 5 (1972), 361–372.
55. Klein, G.; Jiang, J.J.; and Cheney, P. Resolving difference score issues in information systems research. *MIS Quarterly*, 33, 4 (2009), 811–826.
56. Lee, Y. Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50, 2 (2011), 361–369.
57. Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; and Yuan, X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, (2019), 13–24.
58. Lindell, M.K., and Whitney, D.J. Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86, 1 (2001), 114–121.
59. Liu, C.W.; Huang, P.; and Lucas, H.C. Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems*, 37, 3 (2020), 758–787.

60. Lowry, P.B., and Moody, G.D. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, 25, 5 (2015), 433–463.
61. MacKenzie, S.B. Opportunities for improving consumer research through latent variable structural equation modeling. *Journal of Consumer Research*, 28, 1 (2001), 159–166.
62. Malhotra, N.K.; Kim, S.S., and Patil, A. Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, 52, 12 (2006), 1865–1883.
63. Milne, S.; Orbell, S.; and Sheeran, P. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, 7-May, (2002), 163–184.
64. Moody, G.D.; Galletta, D.F., and Lowry, P.B. When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications*, 13, 4 (2014), 266–282.
65. Moody, G.D.; Siponen, M.; and Pahlila, S. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42, 1 (2018), 285–311.
66. Nordgren, L.F.; van Harreveld, F., and van der Pligt, J. Ambivalence, discomfort, and motivated information processing. *Journal of Experimental Social Psychology*, 42, 2 (2006), 252–258.
67. Petrescu, M. Marketing research using single-item indicators in structural equation models. *Journal of Marketing Analytics*, 1, (2013), 99–117.
68. Plambeck, N., and Weber, K. CEO ambivalence and responses to strategic issues. *Organization Science*, 20, 6 (2009), 993–1010.
69. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; and Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88, 5 (2003), 879–903.
70. Priester, J.R., and Petty, R.E. Extending the bases of subjective attitudinal ambivalence: Interpersonal and intrapersonal antecedents of evaluative tension. *Journal of Personality and Social Psychology*, 80, 1 (2001), 19–34.
71. Richardson, H.A.; Simmering, M.J.; and Sturman, M.C. A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, 12, 4 (2009), 762–800.
72. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91, 1 (1975), 93–114.
73. Rogers, R.W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J.T. Cacioppo and R.E. Petty, (eds.), *Social Psychophysiology: A Sourcebook*. New York, US: Guilford, 1983, pp. 153–176.
74. Roscoe, J.; Subin, S.; and Acosta, C.M. More than 40,000 university of Maryland email addresses are for sale on the dark web. *The Diamondback*, 2017. <http://www.dbknews.com/2017/04/06/umd-stolen-fake-student-emails/>.
75. Roster, C.A., and Richins, M.L. Ambivalence and attitudes in consumer replacement decisions. *Journal of Consumer Psychology*, 19, 1 (2009), 48–61.
76. Rothman, N.B.; Pratt, M.G.; Rees, L.; and Vogus, T.J. Understanding the dual nature of ambivalence: Why and when ambivalence leads to good and bad outcomes. *Academy of Management Annals*, 11, 1 (2017), 33–72.
77. Schuetz, S.W.; Lowry, P.B.; Pienta, D.A., and Thatcher, J.B. The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, 37, 3 (2020), 723–757.
78. Silic, M., and Lowry, P.B. Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, 37, 1 (2020), 129–161.
79. Sommestad, T.; Karlzén, H.; and Hallberg, J. A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security*, 9, 1 (2015), 26–46.

80. Sparks, P.; Harris, P.R.; and Lockwood, N. Predictors and predictive effects of ambivalence. *British Journal of Social Psychology*, 43, (2004), 371–383.
81. Spears, J.L., and Barki, H. User participation in information systems security risk management. *MIS Quarterly*, 34, 3 (2010), 503–522.
82. Stein, M.-K.; Newell, S.; Wagner, E.L.; and Galliers, R.D. Coping with information technology: Mixed emotions, vacillation, and nonconforming use patterns. *MIS Quarterly*, 39, 2 (2015), 367–392.
83. Tanner, J.F.J.; Hunt, J.B., and Eppright, D.R. The protection motivation model: A normative model of fear appeals. *Journal of Marketing*, 55, 3 (1991), 36–45.
84. Thompson, M.M., and Zanna, M.P. The conflicted individual: Personality-based and domain-specific antecedents of ambivalent social attitudes. *Journal of Personality*, 63, 2 (1995), 259–288.
85. Thompson, M.M.; Zanna, M.P.; and Griffin, D.W. Let's not be indifferent about (attitudinal) ambivalence. In R.E. Petty and J.A. Krosnick, (eds.), *Attitude Strength: Antecedents and Consequences*. Mahwah: Erlbaum, 1995, pp. 361–386.
86. Thompson, N.; McGill, T.J.; and Wang, X. Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, (2017), 376–391.
87. Thurstone, L.L., and Chave, E.J. *The Measurement of Attitude*. Chicago, US: University of Chicago Press, 1929.
88. Torten, R.; Reaiche, C.; and Boyle, S. The impact of security awareness on information technology professionals' behavior. *Computers & Security*, 79, (2018), 68–79.
89. Vance, A.; Siponen, M., and Pahnla, S. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49, 3-4 (2012), 190–198.
90. Venkatesh, V.; Aloysius, J.A.; Hoehle, H.; and Burton, S. Design and evaluation of auto-ID enabled shopping assistance artifacts in customers' mobile phones: Two retail store laboratory experiments. *MIS Quarterly*, 41, 1 (2017), 83–117.
91. Venkatesh, V., and Goyal, S. Expectation disconfirmation and technology adoption: Polynomial modeling and response surface analysis. *MIS Quarterly*, 34, 2 (2010), 281–303.
92. Venkatesh, V., and Morris, M.G. Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, 24, 1 (2000), 115–139.
93. Venkatesh, V.; Morris, M.G.; Davis, G.B.; and Davis, F.D. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27, 3 (2003), 425–478.
94. Warkentin, M.; Johnston, A.C.; Shropshire, J.; and Barnett, W.D. Continuance of protection security behavior: A longitudinal study. *Decision Support Systems*, 92, (2016), 25–35.
95. Weir, C.S.; Douglas, G.; Carruthers, M.; and Jack, M. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28, 1–2 (2009), 47–62.
96. Zhao, X.; Lynch, J.G.; and Chen, Q. Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, 37, 2 (2010), 197–206.