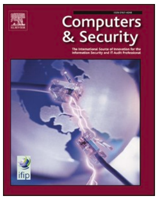
Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose



"No point worrying" – The role of threat devaluation in information security behavior

Nik Thompson [*], Tanya McGill, Nidhi Narula

Curtin University, Kent Street, Bentley, Western Australia, 6102, Australia

ARTICLE INFO

Keywords:
Information security
Threat devaluation
Emotion-focused coping
Problem focused coping
Phishing

ABSTRACT

Extant information security research is characterized by a focus on problem-focused security behaviours, while overlooking the internal, and emotion-focused coping responses that humans exhibit. Threat devaluation, where severity is downplayed, is an established dimension of risk perception, and yet it has not been considered in information security research to date. We address this gap by developing and empirically testing a research model of how threat and coping factors from Protection Motivation Theory influence both problem-focused and emotion-focused coping responses. Data was collected from 518 users and PLS was used to reveal the determinants of, and the relationship between, problem-focused and emotion-focused coping behaviors. The results demonstrate that threat devaluation is a measurable outcome of all threat and coping appraisals considered, providing evidence that multiple coping strategies may be involved in a security threat situation. We also find that many of the well-established determinants of information security behavior, such as self-efficacy, are significantly related to emotion-focused responses. This has implications for researchers and practitioners who seek to create secure environments where users are more likely to enact constructive and problem-focused security behaviors.

1. Introduction

A significant body of research has examined a range of factors that potentially influence the intentions of users to protect against information security threats; that is, to undertake task-centered problem-focused coping (PFC). Theories such as Protection Motivation Theory (PMT) (Rogers, 1975) and Technology Threat Avoidance Theory (TTAT) (Liang and Xue, 2009) build upon work in the health sciences domain and have proved to be effective theoretical models for understanding information security behaviors. As a result, these theories have been well received by the information systems community and form the basis of a large proportion of behavioral information security research. Such models typically include constructs to model perceptions of threat severity and likelihood, as well as the efficacy of both the self and any protective measures. These leading models of information security behavior consider users' protection motivation and protective behavior and have proved valuable in explaining PFC behaviors in the context of information security.

However, recent research in information security has revealed that users also respond to threats with a range of emotion-focused coping (EFC) responses. For example, users may not believe that the risk of malware applies to them (wishful thinking) or may deny that reuse of passwords could lead to identity theft (denial). As such, prevalent behavioral information security models fail to fully consider the affective and emotional context and do not accommodate users who may cope with a threat in a way that does not involve protective behavior.

Coping has been defined as “the cognitive and behavioral effort to manage specific external and/or internal demands that are appraised as taxing or exceeding the person’s resources” (Lazarus and Folkman, 1984, p. 141). According to this definition, it is possible that the effort a user exerts toward managing a challenging (information security) situation need not be directly problem-focused but may instead be inwardly focused on managing the associated emotional impact of the threat. Coping responses may thus be categorized into EFC and PFC.

Multiple EFC responses have been identified and associated with various outcomes both in health-related domains (e.g. Carver et al., 1989; Folkman, 1988) and in the information security literature (e.g. Liang et al., 2019). Emotion-focused responses have been further categorized as outward and inward EFC responses (Liang et al., 2019), with inward EFC responses such as denial (Xin et al., 2021) and avoidance

[*] Corresponding author.
E-mail address: nik.thompson@curtin.edu.au (N. Thompson).

https://doi.org/10.1016/j.cose.2024.103897
Received 18 September 2023; Received in revised form 16 January 2024; Accepted 8 May 2024
Available online 21 May 2024

(Liang et al., 2019) being regarded as potentially counterproductive as they can hinder adoption of PFC responses, whereas outward focused EFC responses such as venting and social support can help users achieve the emotional state they require to engage in PFC (Liang et al., 2019).

Threat devaluation is an emotion-focused response that was explored in the health context by Davey (1993), who described it as a response that acknowledges that the problem or threat exists, but attempts to reduce its stressfulness. For example, in the security context, when a user is aware that email phishing is prevalent but devalues the threat they face and believes that they do not currently need to take the threat too seriously, they are engaging in threat devaluation. The threat is not ignored but neither is the need for urgent action perceived. Davey (1993) found that, unlike denial, threat devaluation can be associated with PFC when dealing with health stresses, such that it is a response used with threats that are perceived as relatively controllable and allows individuals to preserve their attention for more major threats.

Understanding more about threat devaluation and the role it might play in user responses to information security threats is important because of the differing influences that inward and outward EFC responses can have on PFC (Liang et al., 2019; Xin et al., 2021). If threat devaluation proves to play a similar role to outward EFC responses such as social support, it may ultimately contribute to PFC, but if it proves to be more similar to inward responses such as denial, it may impede PFC. Knowing this, and knowing which factors influence it, should provide information security practitioners with information that helps them to understand the emotional state of users and to support users as they face security threats, both directly and via training and awareness campaigns.

To date, no previous published research has considered whether threat devaluation plays a role in responses to information security threats. This paper addresses this lack of prior work. The phishing domain was chosen for this research as phishing is an increasingly important security issue with the Anti-Phishing Working Group (2022) reporting more than 4.7 million attacks in 2022, yet users may see it as a threat that is controllable (Liang and Xue, 2009; Verkijika, 2019). We build on the work of Liang et al. (2019), who considered the roles of different types of EFC in problem-focused information security behavior and propose and test a model of the potential role that threat devaluation plays in users' responses to phishing threats. The study addresses two research questions in the context of phishing threats:

RQ1: How is threat devaluation influenced by the factors that have been found to influence PFC behavior?

RQ2: How does threat devaluation influence PFC behavior?

2. Literature review

2.1. Phishing

Phishing employs a combination of social engineering and technical measures to steal the financial and personal information of users. Common protections against phishing include the anti-phishing toolbars that are available for browsers and anti-phishing software tools; these provide visual warnings and alerts when a suspected phishing website is detected. Though such tools and techniques are well established to safeguard against this information security threat, the number of phishing victims continues to increase (Anti-Phishing Working Group, 2022). Addressing the threat of phishing has, therefore, become a significant area of information security research (e.g., Arachchilage et al., 2016; Bax et al., 2021; Williams and Joinson, 2020), and several key findings from the broader information security research domain have been successfully applied in this context.

Much of the behavioral information security research on phishing has considered the role that coping and threat appraisal play in influencing protection motivation by using and extending theories such as PMT (Rogers, 1983) and TTAT (Liang and Xue, 2009). Research based on these theories has demonstrated the roles of perceived vulnerability, perceived severity, self-efficacy, response efficacy, and response cost in determining the extent to which users take protective action against phishing threats (Arachchilage and Love, 2013; Bax et al., 2021; Jansen and van Schaik, 2018). However, recent research has highlighted that as well as PFC, generally investigated in terms of protection motivation and protective behavior undertaken, users also respond to information security threats with a range of emotion-focused responses (Chen and Liang, 2019; Liang et al., 2019; Wang, Li, and Rao, 2017; Xin et al., 2021). Therefore, a greater understanding of the role of other modes of coping with phishing threats is needed.

2.2. Coping

Lazarus and Folkman (1984) distinguished between two fundamental types of coping with stress: problem-focused, and emotion-focused. They define PFC as responses that aim to manage or alter the problem, whereas EFC aims to regulate emotional responses to the problem. In PFC, when being faced with a threat, a user responds in a manner that deals directly with the threat. In the information security domain, the following are examples of labels given to forms of PFC: protection behavior (Bax et al., 2021), task-focused coping (Wang et al., 2017), and information security policy compliance (Chen et al., 2021). EFC strategies can be considered inward or outward focused (Liang et al., 2019), where inward EFC acts to suppress negative emotions by ignoring or distorting the perception of information security threats. Several different types of inward EFC have recently been considered in information security research, including denial (Liang et al., 2019), wishful thinking (Liang et al., 2019; Xin et al., 2021), and avoidance (Chen and Zahedi, 2016; Moody et al., 2018; Xin et al., 2021). Outward EFC responses work to reduce the negative effects of stressful situations by directly regulating the emotions generated by threats but do not deliberately change how the threat is perceived. Outward EFC responses that have been investigated in recent information security research include venting and seeking emotional support (Liang et al., 2019).

In the health domain, Lazarus and Folkman (1984) considered that the controllability of the threat determined the extent to which there was a greater preference for PFC or EFC, with controllable situations being more associated with problem-focused responses and more extensive use of EFC responses in uncontrollable situations.

The categorization of coping as either just problem-focused or just emotion-focused has also been examined, and in some cases criticized as an oversimplification, including by Lazarus (e.g., Compas et al., 2001; Lazarus, 1996; Skinner et al., 2003). Similarly, Liang and Xue (2009) argue that in the information security domain, individuals engage in both PFC and EFC. It is also possible that a single coping response may address both the problem and emotions (Compas et al., 2001).

Liang et al. (2019) considered EFC responses to be antecedents of PFC and tested a model of how inward and outward types of EFC influence security behavior. They found that inward EFC had a negative influence on PFC behavior and that outward EFC had a weak positive effect on PFC behavior, concluding that outward EFC can promote improved information security behavior.

2.3. Threat devaluation

Threat devaluation is a form of EFC where the threat is recognized, but in response, its severity is devalued to relieve stress. Davey (1993) is one of the few authors to discuss the role of threat devaluation as a coping strategy, and his work was in the health domain. In this context Davey compares threat devaluation firstly with denial, a form of inward EFC in which an individual tries to deny that the problem is threatening or relevant, and also with positive reappraisal, in which the threat is reappraised to have positive value (e.g., by considering it a “challenge”). The role of threat devaluation in information security has not yet been investigated; hence this paper proposes and tests a model of the potential role that threat devaluation plays in responses to phishing threats.

Threat devaluation differs from denial in that the individual accepts that the threat exists but attempts to reduce the stress associated with it. It differs from positive reappraisal in that there is no attempt to see the problem as a positive challenge. In the health context, Davey (1993) found threat devaluation to be positively correlated with more problem-focused responses to threats and presented several possible reasons for this. He argued that threat devaluation may involve an appraisal process that allows individuals to temporarily deflect attention from less important problems to facilitate attention to more serious threats. He also suggested that it might provide a breathing space that allows the individual to prepare to cope with the threat; that is, the threat is not denied, but devalued sufficiently to allow space before addressing it. In an information security context, this might occur when a user is concerned about the threat of malware, but initially has an emotional response that downplays the threat, and they thus delay taking action such as updating their antivirus software. Given these characteristics, threat devaluation may be classified as an outward form of EFC, however, it differs from the forms described by Liang et al. (2019): emotional support seeking and venting.

Davey initially argued that threat devaluation may be appropriate when the threat is perceived as uncontrollable, but this was disproved in a second study, which found that threat devaluation was more likely to occur in controllable situations (Davey, 1993). In the information security context, this sense of controllability is formed based on the perceived effectiveness and costs of the available protective measures and on the user's confidence in their ability to successfully perform these measures (Liang and Xue, 2010). Liang et al. (2019) found that when users believed that they were in control of an information security threat, they were less likely to use forms of inward EFC to cope. However, they still needed outward EFC to deal with the emotions associated with the stressful situation. Phishing is a large problem (Anti-Phishing Working Group, 2022) but approaches exist to counter it, and the perceptions of users about it are influenced by factors such as their phishing awareness and their beliefs about anti-phishing tool usefulness (Abbasi et al., 2016). Therefore, users may see it as a relatively controllable information security threat and hence threat devaluation may play a role in their responses to the threat.

3. Model and hypotheses

The Extended Parallel Process Model (EPPM) (Witte, 1992, 1994) draws from PMT (Rogers, 1983) and the Parallel Response Model (Leventhal, 1970, 1971). It includes the PMT concepts of vulnerability to a threat and the severity of a threat as influences on an individual's emotional response to the threat (i.e., fear). It also includes consideration of the efficacy of a protective action (response efficacy), and the belief in one's ability to perform the action required (self-efficacy). Each of these then influences the response to the threat, which can be an effort to control or limit the level of the threat (protection motivation) or to counter or inhibit the individual's emotional response to the threat (defensive motivation). EPPM was developed to explain success and failure in coping with threats by capturing the interplay of fear control and danger control. The model tested in this study uses both PMT and EPPM as a starting point to represent the potential role of threat devaluation in responses to phishing threats (see Fig. 1). Table 1 provides definitions of the constructs in the model.

PMT (Rogers, 1983) and EPPM (Witte, 1992, 1994) both propose that perceived severity and perceived vulnerability influence fear. These

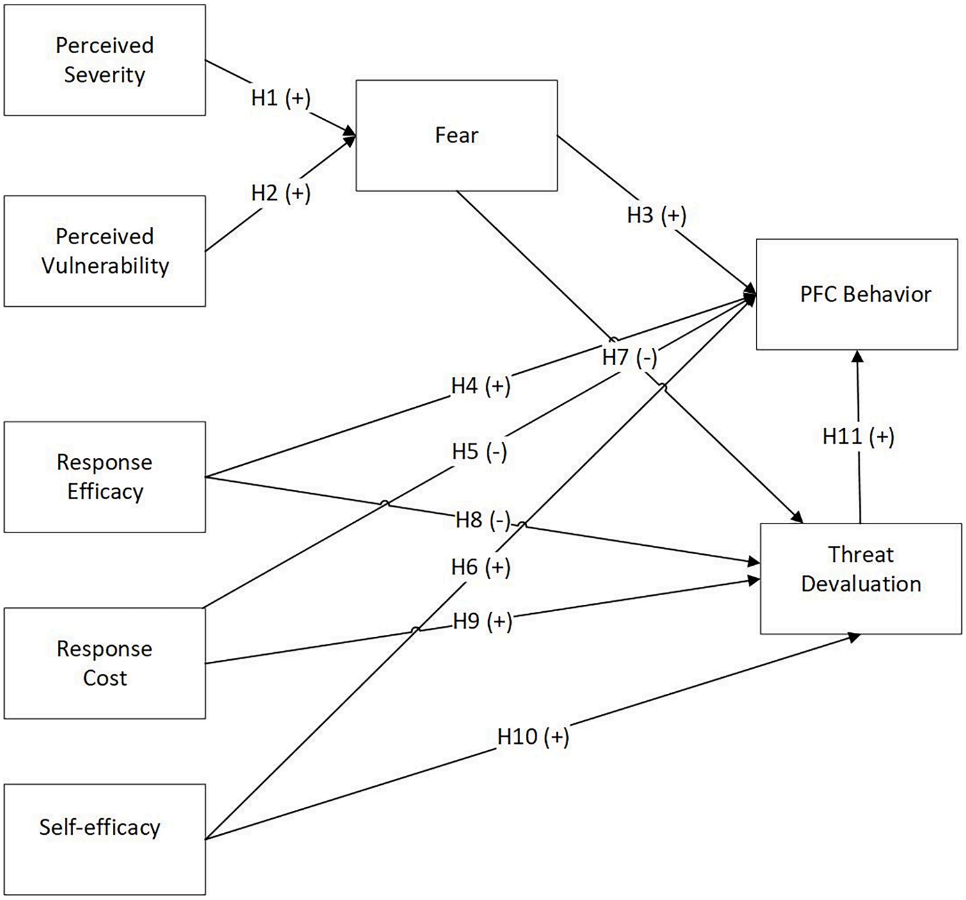


Fig. 1. Research model.

Table 1
Construct definitions.

Construct	Definition
Perceived severity	Perceived severity is defined as an individual's perception of the seriousness of the consequences of falling victim to a phishing threat.
Perceived vulnerability	Perceived vulnerability is defined as an individual's perception of the likelihood of falling victim to a phishing threat.
Fear	Fear can be described as an emotional feeling about threat. With respect to phishing threats, fear might manifest as nervousness or anxiety about potential dangers and reluctance to open emails because of the potential threat.
Response efficacy	Response efficacy is the extent to which an individual believes that the recommended actions will effectively mitigate or eliminate the threat.
Self-efficacy	Self-efficacy refers to an individual's beliefs about how successfully they will be able to perform the protective behaviors to avoid falling victim to a phishing attack.
Response cost	Response cost is the perceived opportunity cost that an individual believes is associated with taking protective action against phishing threats (e.g., time, effort, or financial).
PFC behavior	Problem-focused responses to a threat occur when, upon being faced with a threat, an individual responds in a manner that deals directly with the threat to protect them from the possible damage caused by the threat. In this study, PFC behavior is defined as the extent to which an individual uses appropriate protective measures to counter phishing threats. For example, PFC behavior might involve carefully assessing e-mails before opening them or before clicking on the links and acting on warnings from anti-phishing tools.
Threat devaluation	Threat devaluation is a coping response where the threat is recognized but it is devalued to relieve stress (Davey, 1993). In the context of phishing threats, threat devaluation refers to an individual potentially underestimating the impact of a phishing attack to reduce their stress, thus allowing themselves to not immediately undertake protective behavior.

threat appraisal factors have been shown to positively influence fear in a range of information security domains (e.g., Boss et al., 2015; Liang and Xue, 2010; Mwagwabi et al., 2018). Perceived severity and perceived vulnerability have also been shown to influence fear in the phishing domain (Arachchilage and Love, 2013; Bax et al., 2021; Jansen and van Schaik, 2018); that is, as a user perceives an email phishing threat to be more serious, or themselves to be more vulnerable to this threat, they will have a greater emotional response to it. Therefore, we hypothesize that:

H1. Perceived severity of phishing threats positively influences fear.

H2. Perceived vulnerability to phishing threats positively influences fear.

Fear is central to the EPPM (Witte, 1994) and the revised PMT (Rogers, 1983), which suggest that when a threat is deemed relevant, fear is invoked, and in response, the user takes action. The relationship between fear and security behavior or the intention to undertake it has been supported in some information security research (e.g., Boss et al., 2015; Chen et al., 2022; Liang and Xue, 2010; Liang et al., 2019; Mwagwabi et al., 2018), including when users are faced with phishing threats (Arachchilage and Love, 2013; Bax et al., 2021). Therefore, an increase in an individual's level of fear about email phishing threats should result in an increase in their PFC behavior in response to the phishing threat, and the following is hypothesized:

H3. Fear positively influences PFC behavior.

The perceived efficacy of potential responses is proposed to influence the intention to perform protective behaviors (Rogers, 1983; Witte, 1992, 1994), and consequently protective behavior. Many information security studies have provided support for this (e.g., Boss et al., 2015; Chen et al., 2022; Liang and Xue, 2010; Mwagwabi et al., 2018; Xin et al., 2021). Users can protect themselves against phishing by carefully checking emails as well as using anti-phishing toolbars in browsers and anti-phishing software that provide visual warnings and alerts when a potential phishing website is identified. In the phishing domain, increases in perceptions of the efficacy of these and other responses are associated with increases in intentions to perform protections against phishing threats (Arachchilage and Love, 2013; Bax et al., 2021; Shahbaznezhad et al., 2020; Williams and Joinson, 2020); therefore, we hypothesize:

H4. Response efficacy positively influences PFC behavior.

Response costs are those that users perceive are associated with taking protective actions; they include not only financial costs but also the time, effort, and inconvenience that these may involve. The revised PMT (Rogers, 1983) represents response costs as an inhibitor of intentions to perform protective behaviors, and some previous information security research supports this (Boss et al., 2015; Chenoweth et al., 2009; Liang and Xue, 2010; Thompson et al., 2017). However, some studies have not found response costs to play a role (e.g., Boehmer et al., 2015; Mwagwabi et al., 2018).

As with research on its role in responses to other information security issues, the results about response costs associated with protecting against phishing threats have not always been consistent. Although Jansen and van Schaik (2018) did not find this to be the case, both Arachchilage and Love (2013) and Bax et al. (2021) demonstrated that response costs can play a role in protection against phishing threats; that is, these studies suggest that when users perceive the cost of protecting themselves against phishing threats to be higher, they are less likely to be motivated to protect themselves. We hypothesize that:

H5. Response cost negatively influences PFC behavior.

Self-efficacy is another important coping appraisal factor proposed to influence the intention to perform protective behaviors (Rogers, 1983; Witte, 1992, 1994). Previous research has provided consistent support for this in many information security contexts, where users' belief in their ability to successfully perform the recommended protective behaviors has positively influenced either their intention to do so and/or the extent to which they do so (Belanger and Crossler, 2019; Mills and Sahai, 2019; Thompson et al., 2017; Warkentin et al., 2016). However, Xin et al. (2021) did not find that self-efficacy played a role in PFC when facing mobile malware threats. In previous studies of phishing security behavior, increases in self-efficacy have been associated with increases in intentions to protect against phishing threats (Arachchilage and Love, 2013; Bax et al., 2021; Jansen and van Schaik, 2018; Williams and Joinson, 2020); therefore, the following hypothesis is proposed:

H6. Self-efficacy positively influences PFC behavior.

Whilst there is evidence that fear is associated with adaptive responses such as improved password behavior (Mwagwabi et al., 2018), intention to use anti-malware software (Boss et al., 2015), and protecting against phishing threats (Bax et al., 2021), less research has considered the relationship between fear and EFC in an information security context. Several recent studies have started to explore the role of different emotion-focused responses to fear (e.g., Chen and Liang, 2019; Cho et al., 2020; Liang et al., 2019; Xin et al., 2021). Cho et al. (2020) demonstrated that fear associated with online privacy risks had a positive association with inward EFC responses such as avoidance and disengagement. Similarly, Liang et al. (2019) found that fear of external security threats positively influenced several inward EFC responses including denial and wishful thinking, and also positively influenced the two forms of outward EFC they considered: venting and seeking social support. However, given the finding of Davey (1993) that threat devaluation is positively associated with problem-focused responses to threats in situations where the threat is perceived as controllable, we argue that users can regard phishing as a potentially controllable threat. Thus, when fear of this threat is lower, they may employ threat devaluation as a response that buys time before engaging in protective behavior. However, users with higher fear are less likely to engage in this response. We therefore hypothesize that:

H7. Fear negatively influences threat devaluation.

Chen et al. (2022) considered both self-efficacy and response efficacy as components of perceived coping efficacy and explored their role in avoidance in response to internet security attacks. Increased perceptions of perceived coping efficacy were associated with decreased avoidance. That is, when users believed that the responses were effective, they were less likely to adopt this inward emotion-focused response. Xin et al. (2021) investigated how response efficacy influences five kinds of EFC and found that all except avoidance were negatively influenced by increases in response efficacy.

Despite the finding of Liang et al. (2019) that perceived avoidability, a construct that partially captures response efficacy, had no relationship with venting and seeking emotional support we propose that response efficacy has a negative relationship with threat devaluation such that the more users believe in the efficacy of responses to phishing threats the less need there is for them to employ this strategy to control their emotions and hypothesize:

H8. Response efficacy negatively influences threat devaluation.

The cost of responding to information security threats (e.g., in terms of time, effort, and money) has been shown to negatively impact intentions to take protective action (Boss et al., 2015; Chenoweth et al., 2009; Liang and Xue, 2010; Thompson et al., 2017). However, less is known about the potential impact of response costs on EFC. In a study on intention to use anti-spyware protection (Chenoweth et al., 2009), response cost was the only coping appraisal factor to influence EFC (described as maladaptive coping), and it had a positive influence. That is, the higher the perceived cost of the recommended response the more likely users were to respond in a way that did not deal directly with the threat. Similarly, Marett et al. (2011) found response costs positively influenced two EFC responses: avoidance and hopelessness. In a phishing-specific study, Bax et al. (2021) also showed that increases in response cost were associated with increases in maladaptive behavior. Consistent with Davey (1993) we propose that in situations where the cost of responding to phishing threats is perceived by users to be high, they are more likely to engage in threat devaluation to allow themselves time before engaging in problem-focused responses, we therefore hypothesize that:

H9. Response cost positively influences threat devaluation.

As discussed above, Chen et al. (2022) found that increases in self-efficacy (as well as perceived response efficacy) reduced levels of avoidance in response to internet security attacks. Chen and Zahedi (2016) also found a weak negative effect of self-efficacy on avoidance but suggest that there may be cultural differences in the role played by self-efficacy, with it playing more of a role with US users than Chinese users. However, Xin et al. (2021) found that self-efficacy did not influence any of the forms of EFC they investigated in response to mobile device malware threats and similarly, it did not influence maladaptive coping in Chenoweth et al. (2009). Therefore, more research on the relationship between self-efficacy and EFC is needed. In this study, we argue that because threat devaluation appears to be important in situations that are perceived as controllable (Davey, 1993), and phishing has recommended responses, users who believe that they will be able to undertake recommended protective actions are more likely to engage in threat devaluation as it provides mental space that allows them to prepare to cope with the threat. In this study, we hypothesize that:

H10. Self-efficacy positively influences threat devaluation.

The relationship between EFC and PFC has been considered in several information security studies, and the results suggest that increases in some types of inward types of EFC are associated with reductions in security behavior intentions and some types of PFC; for example, denial, psychological distancing, and wishful thinking (Liang et al., 2019) and avoidance and fatalism (Xin et al., 2021). However, in Xin et al. (2021) reactance, hopelessness, and wishful thinking did not have significant impacts on PFC behavior. Liang et al. (2019) also investigated the relationship between outward EFC and PFC behavior and found that outward EFC had a weak positive influence on PFC behavior. Given this finding in the information security domain and the fact that Davey (1993) found the use of threat devaluation to be positively correlated with problem-focused responses to threats in the health context, we propose that users are more likely to employ PFC responses to address phishing threats when they have higher levels of threat devaluation and hypothesize:

H11. Threat devaluation positively influences PFC behavior.

4. Method

The population of interest for this study is Australian adult users who are exposed to potential phishing threats. Phishing attacks aim to steal data, especially the user's personal information, including login credentials and passwords to various online accounts, therefore online data collection was an appropriate mechanism to reach the desired group of respondents and an online questionnaire was used to collect data to test the research model. Human research ethics approval to conduct the research was obtained prior to the collection of data.

Participants were recruited using the third-party survey company, PollFish (www.pollfish.com). Pollfish conducted the screening for demographic requirements (i.e., potential participants needed to be over 18 years of age and located in Australia) and invited suitable members of their survey panels. Invitees received a detailed participant information sheet, and link to the questionnaire and could proceed after consenting. The invitation also included an e-mail address for any queries relating to the research. The data was collected between late October 2021 and early April 2022.

The online questionnaire was created using Qualtrics. The items to measure the constructs in the proposed model were drawn from previous information security research where possible and were adapted for the phishing domain if necessary. These items were all measured on 5-point Likert scales from 'Strongly Disagree' to 'Strongly Agree'. As all the constructs in the model were measured through self-reports, common method bias (CMB) was possible. To reduce this risk, we used the procedural remedies of protecting the anonymity of the respondents to minimize the evaluation apprehension (Podsakoff et al., 2003) and improving measurement items through careful construction (Podsakoff et al., 2012), as item ambiguity has been identified as a common problem in the comprehension stage of response (Tourangeau et al., 2000). The clarity and conciseness of the questionnaire were examined in pilot testing with ten members of the target population and based on their feedback slight changes were made to the wording of several items. Table A.1 includes the items and their sources.

The proposed model was tested using partial least squares (PLS). PLS is a second-generation statistical technique that is well suited for theory development such as the new model proposed in this research (Lowry and Gaskin, 2014). The model was tested in two stages using SmartPLS (Ringle et al., 2005). We first evaluated the measurement model and then the structural model. Bootstrap resampling using 5000 samples was used to determine the significance of the paths in the structural model.

5. Results

We received a total of 518 valid responses (54.8 % female and 45.2 % male) to the questionnaire. Table 2 shows the distribution of participants by gender, age, and education.

Before testing the model, we conducted two statistical tests to examine whether CMB was a problem. Using the Harman one-factor test

Table 2
Participant background information.

		Percent
Gender	Female	54.8
	Male	45.2
Age	18–24	25.7
	25–34	26.6
	35–44	20.5
	45–54	9.6
	55 and above	17.6
Highest education level	Primary school	6.5
	High school	27.3
	Vocational qualification	28.9
	Undergraduate	24.5
	Postgraduate	12.8

(Podsakoff et al., 2003), the amount of variance explained by the first factor was 18.80 %, well below the recommended threshold of 50 %. Next, we conducted a correlational marker variable test (Lindell and Whitney, 2001), which showed that, after controlling for a marker variable (measured on the same scale but theoretically distinct), all originally significant correlations remained significant. Given these results, and the procedural strategies reported in Section 4, CMB was unlikely to be a serious concern in this research.

The measurement model was assessed for internal consistency, convergent validity, and discriminant validity. Internal consistency was assessed using composite reliability (CR) and all constructs had values above 0.70 as recommended by Hair et al. (2017). Outer loadings and average variance extracted (AVE) were used to assess convergent validity. Each item loaded significantly on its construct; however, several item loadings were not above the recommended 0.708 (Hair et al., 2017) and were investigated further and considered for removal to improve AVE (Table A.1 identifies items that were removed from the analysis). The final AVE for all constructs was above the minimum threshold value of 0.5 (Hair et al., 2017). Table 3 provides the final CR and AVE for each of the constructs in the proposed model. As can be seen, both internal consistency and convergent validity are satisfactory.

Discriminant validity was initially assessed using both cross loadings and the Fornell-Larcker criterion. All measurement items were found to load more highly on their own construct than on any other construct. The square root of AVE for each construct was also greater than the correlation between that construct and any other construct (see Table A.2). Discriminant validity was therefore demonstrated with both approaches. In addition, we conducted a further test of discriminant validity using the heterotrait–monotrait ratio (HTMT) of correlations criterion. The HTMT ratios presented in Table A.3 are all under the threshold of 0.90 (Henseler et al., 2015), further demonstrating that our data did not suffer from discriminant validity issues.

The structural model was examined next. Fig. 2 summarizes the results of this evaluation. Nine of the 11 hypotheses were supported. The model explained 23 % of the variance in fear ($R^2 = 0.23$), 38 % of the variance in PFC behavior ($R^2 = 0.38$) and 29 % ($R^2 = 0.29$) of the variance in threat devaluation.

Both perceived severity and perceived vulnerability had a positive influence on fear ($\beta = 0.34$, $p < 0.001$ and $\beta = 0.24$, $p < 0.001$). This provided support for H1 and H2. H3 was also supported as fear had a positive influence on PFC behavior ($\beta = 0.30$, $p < 0.001$). Consistent with PMT (Rogers, 1983) and EPPM (Witte, 1992, 1994), increases in response efficacy and self-efficacy led to increases in PFC behavior ($\beta = 0.20$, $p < 0.001$ and $\beta = 0.25$, $p < 0.001$), providing support for H4 and H6. However, response cost was not found to influence PFC behavior as hypothesized ($\beta = -0.06$, $p = 0.06$); therefore, H5 was not supported.

Table 3
Convergent validity and AVE values.

Construct	CR	AVE
Fear	0.80	0.50
Perceived severity	0.90	0.63
Perceived vulnerability	0.80	0.51
PFC behavior	0.81	0.59
Response cost	0.80	0.50
Response efficacy	0.81	0.52
Self-efficacy	0.80	0.50
Threat devaluation	0.81	0.52

Hypotheses H7 to H10 relate to potential impacts on threat devaluation. Consistent with H7, as fear increased threat devaluation decreased, and therefore H7 was supported ($\beta = -0.29$, $p < 0.001$). As proposed, increases in response efficacy led to decreases in threat devaluation ($\beta = -0.12$, $p = 0.004$) and increases in response cost led to increases in threat devaluation ($\beta = 0.43$, $p < 0.001$). Both H8 and H9 were, therefore, also supported.

The model tested in this research proposes that as users' self-efficacy for managing phishing threats increases, their use of threat devaluation as a coping strategy also increases. This was found to be the case, as a weak positive relationship was identified between self-efficacy and threat devaluation ($\beta = 0.09$, $p = 0.022$); H10 was therefore supported.

Hypothesis H11 relates to the relationship between threat devaluation and PFC behavior and proposes that the more that users engage in threat devaluation the more they undertake PFC behavior in response to phishing threats. However, threat devaluation was not found to influence PFC behavior ($\beta = -0.02$, $p = 0.335$) and, therefore, H11 was not supported. The testing of the hypotheses is summarized in Table 4 and the results of the structural model testing are summarized below in Fig. 2.

6. Discussion

This research addresses the lack of previous research on the role of threat devaluation in information security behavior. The research is undertaken in the context of protection against phishing threats. Drawing on PMT (Rogers, 1983) and EPPM (Witte, 1992, 1994) and the work of Liang et al. (2019) we propose and test a model of how the threat and coping appraisal factors from PMT influence PFC behavior and threat evaluation and how threat devaluation and PFC behavior are related. The results of this study provide support for nine of the 11 hypotheses.

The first six hypotheses provide some further confirmation of earlier PMT (Rogers, 1983) and TTAT (Liang and Xue, 2009) based studies on user responses to phishing threats. Consistent with previous research (Arachchilage and Love, 2013; Bax et al., 2021), perceived severity and perceived vulnerability positively influenced fear, which influenced PFC behavior. As proposed, both response efficacy and self-efficacy also had direct positive influences on PFC behavior and this is consistent with previous research on phishing (Arachchilage and Love, 2013; Bax et al., 2021; Williams and Joinson, 2020). However, response cost did not influence PFC behavior in this study. Response cost has not been found to consistently influence information security behavior across security contexts (e.g., Boehmer et al., 2015; Mwagwabi et al., 2018) or specifically concerning phishing (e.g., Jansen and van Schaik, 2018), so more research is needed to understand what determines its importance.

Hypotheses H7 to H11 capture the major new contribution of this study in understanding the role threat devaluation plays in user responses to phishing threats. The results demonstrate that fear influences threat devaluation as well as PFC behavior. When individuals have higher levels of fear about phishing threats, they are more likely to take protective action and less likely to engage in threat devaluation. This negative relationship differs from the positive relationships between fear and other forms of both inward and outward EFC identified in previous research; for example, with avoidance and disengagement (Cho et al., 2020), and denial, wishful thinking, venting and seeking social support (Liang et al., 2019).

Since prior work has shown that threat devaluation positively influences problem-focused responses in non-security situations where the

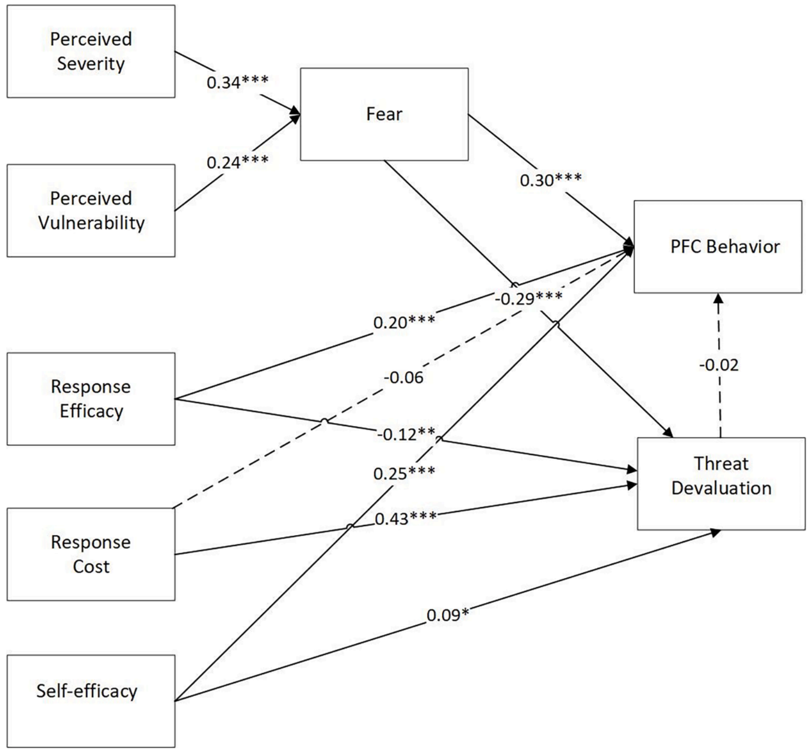


Fig. 2. Model testing results.

Table 4
Summary of hypothesis testing.

	Hypothesis	Result
H1	Perceived severity of phishing threats positively influences fear	Supported
H2	Perceived vulnerability to phishing threats positively influences fear	Supported
H3	Fear positively influences PFC behavior	Supported
H4	Response efficacy positively influences PFC behavior	Supported
H5	Response cost negatively influences PFC behavior	Not Supported
H6	Self-efficacy positively influences PFC behavior	Supported
H7	Fear negatively influences threat devaluation	Supported
H8	Response efficacy negatively influences threat devaluation	Supported
H9	Response cost positively influences threat devaluation	Supported
H10	Self-efficacy positively influences threat devaluation	Supported
H11	Threat devaluation positively influences PFC behavior	Not Supported

threat is perceived as controllable (Davey, 1993), and some users see phishing threats as controllable (Abbasi et al., 2016; Verkijika, 2019), the negative relationship observed between fear and threat devaluation supports our contention that threat devaluation is a response that allows the user to delay their perceived need to take protective action (Davey, 1993). However, this is a strategy that is employed more when fear of the threat is lower, providing a response that allows users to buy time before engaging in protective behavior. Conversely, users with higher fear are less likely to use this response. When fear is higher, users are more likely to adopt problem-focused responses.

As hypothesized, response efficacy negatively influenced threat devaluation. That is, the more that individuals believed in the efficacy of responses to phishing threats the less they used threat devaluation as a response. EFC appeared to be less necessary given the belief in the efficacy of responses to the threat. This is consistent with the findings of Chen et al. (2022) where increased perceptions of perceived coping efficacy (which combines response efficacy and self-efficacy) were associated with decreased avoidance, and with the findings of Xin et al. (2021) where response efficacy had a negative influence on five kinds of EFC.

The perceived cost of responding to phishing threats (e.g., in terms of the time or effort required to address the threat) was proposed to both decrease PFC behavior and increase threat devaluation. As in the phishing related study of Jansen and van Schaik (2018), in this study response cost did not influence PFC behavior. Further research is needed to understand under which circumstance the costs of protection become important determinants of protective behavior. However as proposed, response cost had a positive influence on threat devaluation. This finding is consistent with the results of several previous related studies. In both the Chenoweth et al. (2009) study on intention to use anti-spyware protection and the Marett et al. (2011) research on posting of personal information on social media, increases in response cost were associated with increases in EFC. It seems that when the cost of responding to phishing threats is perceived by users to be high, they are more likely to engage in threat devaluation to allow themselves time before engaging in problem-focused responses.

The role of self-efficacy in users' responses to security threats is clear concerning problem-focused responses, but less so with emotion-focused responses. Although two previous studies have found that self-efficacy has a negative influence on some forms of inward EFC (Chen et al., 2022; Chen and Zahedi, 2016), it did not influence any of the forms of inward EFC considered in Chenoweth et al. (2009) or Xin et al. (2021). No previous research has investigated the role of self-efficacy in outward EFC. The results of this study provide support for our contention that in the phishing domain, users who believe that they have the ability to undertake recommended protective action against phishing threats are more likely to engage in threat devaluation as it provides mental space that allows them to prepare to cope with the threat or give their attention to more urgent matters.

Although several information security studies have found a negative relationship between some forms of inward EFC and PFC (Liang et al., 2019; Xin et al., 2021), Liang et al. (2019) found that outward EFC had a weak positive influence on PFC behavior; hence we hypothesized that this would also be the case when users respond to phishing threats.

However, the results of this study do not support this, and no relationship was found. Outward EFC responses regulate emotions directly and protect emotional stability by changing perceptions of the security threat to protect against negative emotions. Although they share with inward EFC the goal of restoring emotional stability, they differ in terms of how this goal is achieved. Unlike inward EFC, outward EFC should reduce stress whilst still acknowledging the threat and hence assist users to focus on taking protective action. In threat devaluation, this is by providing mental space. The types of outward EFC that Liang et al. (2019) explored were emotion support seeking and venting, not threat devaluation. The results of our study suggest that the role of threat devaluation may not be to increase PFC directly when users are faced with phishing threats, but rather to just reduce their negative emotions without impeding PFC. This is consistent with the third type of protective coping behavior proposed by Pearlin and Schooler (1978), which keeps the emotional consequences of a threat within manageable bounds by perceptually adjusting the meaning of the threat to control its problematic nature. However, in this context, threat devaluation does not appear to also fulfil the first function that Pearlin and Schooler (1978) discuss, the function of eliminating or modifying conditions giving rise to problems, as it does not lead to greater PFC behavior.

Given that Davey (1993) found an association between threat devaluation and problem solving associated with coping in daily life, more research is needed to understand their relationship. This should include investigating the role of context. Although threat devaluation has not previously been studied in any security behavior context, Folkman et al. (1986) and Lazarus (1996) note that contextual factors greatly affect how individuals cope with threat, and previous information security research has shown differing results depending on context. For example, findings on the relationship between perceived vulnerability and problem focussed security behavior have not been consistent across contexts (Mou et al., 2022), with Bax et al. (2021) finding perceived vulnerability important in protection against phishing threats, but it having no role in password protection behavior (Mwagwabi et al., 2018). Similarly, the influence of types of EFC has been shown in different contexts, with avoidance reducing PFC with respect to mobile malware but not with information security policy compliance (Moody et al., 2018).

6.1. Implications for research

Predominant models of information security behavior include measurable or observable security intentions or behaviors as the outcome variable. That is, users either respond to security threats in a practical way, or they are assumed to have taken no response. This modeling thus ignores the range of internal processes that may accompany any threat response in a given context. Our research has highlighted the role of EFC responses, that is, responses that do not directly address the threat but are directed toward regulating the user's internal state. Such internal processes are, by definition, not directly observable and yet can constitute an important determinant of user behavior.

The findings of this study demonstrate that many of the well-understood determinants of security behavior, such as response cost or self-efficacy can also be significant determinants of the emotion-focused responses of the user. This provides evidence that multiple response strategies may be invoked in a security threat situation, and that there is potential that some of the otherwise un-explained actions of users may be attributed to these internal and unobservable responses. The threat devaluation response that was investigated in this study was not found to have a direct influence on the ultimate PFC actions that a user may take in addressing phishing threats, but its potential role in responses to other information security threats that users may consider relatively controllable should be investigated. Future research should also build on this study by considering the roles of the other dimensions of EFC that have been identified in prior work. Models such as PMT (Rogers, 1983) remain instrumental in behavioral research, yet the ability of such models to explain the variance of outcome variables is an aspect that researchers consistently slate for improvement. Information security scholars continue to extend and improve these basic and foundational models with new constructs, seeking to understand the sources of this unexplained variance in user security behaviors. A significant research implication arising from this research is thus to provide justification for researchers to consider EFC responses in their modeling, including other dimensions such as avoidance behaviors. We also present a validated survey instrument to measure the new construct of threat devaluation, as this has not before been measured in prior work, and we invite scholars to continue this promising research direction.

Several limitations of the research could also be addressed in future research. First, all of the participants in this study were resident in Australia at the time of data collection. Future research should investigate the generalizability of the findings across other cultures and countries. Also, even though the analysis did not suggest CMB, because all the constructs in the model were measured through self-reports, CMB is possible. Future research on the role of threat devaluation should include further procedural and statistical steps to reduce the potential for this issue. These could include the procedural remedies of minimizing the common scale properties across independent and dependent constructs, including reverse coded items, and increasing the separation of data collection between dependent and independent variables (Jordan and Troth, 2020). Finally, as the research was specific to user responses to phishing threats, the applicability of the model in other security contexts should be confirmed in future research.

6.2. Implications for practice

In terms of practice, the end goal is to enhance security and support users in taking the most secure actions. Evidence-based practitioners may already be well-versed in some of the determinants of security behaviors included in our research model. We now demonstrate that many of these same factors may also affect the internal and emotional state of the user. This is not inherently problematic as it is possible that some EFC responses may lead to increased levels of PFC security behavior (Liang et al., 2019) and hence improved security. However, as this represents a new and little-researched area, there is still a lot to learn in this space. There is the potential that some, particularly inward, EFC responses may diminish or influence the action-oriented behaviors of the user – a prospect that may thus have significant implications for the impact and success of organizational information security initiatives. Security practitioners need to be aware that users do not just have one response to threats. Understanding what the full range of responses might be and how they interact is important to helping users to behave securely and to protect information resources.

Given that many of the same determinants of information security behavior may also evoke EFC, it is reasonable to expect that the (finite) resources of the user may be allocated towards different responses depending on the environment. Indeed, prior work has described a wide range of employee coping strategies (Dewe et al., 2010), although identification of the conditions required to encourage adaptive outcomes has met with limited success (Miller and Kaiser, 2001). The results of this study in the phishing context show that whilst adopting threat devaluation as a coping response did not increase users' PFC behavior, equally it did not reduce it, suggesting that it should not be of concern to practitioners in the way that inward EFC mechanisms such as denial and avoidance should be (Liang et al., 2019; Xin et al., 2021).

Here our goal for practice translates to finding the right conditions to ensure that users favor the PFC pathway instead of devoting resources only to internal coping mechanisms that may reduce protective behavior. However, given that users do not enact just one single coping mechanism (Pearlin and Schooler, 1978), it is important that practitioners understand the range of possible user responses to information security threats. They may then help, via awareness campaigns and training, to reduce the use of inward EFC responses that act against protection (e.g. denial and avoidance), and provide conditions that preferably favor outward EFC that can lead to increased PFC (e.g. social support) or responses such as threat devaluation that do not reduce PFC in the phishing context.

Also, as EFC is more likely in situations of low controllability (D'Arcy et al., 2014), an organizational information technology environment with centralized, inflexible governance may create the precise low-control situation we seek to avoid. Practitioners may seek to empower users to become active participants and decision-makers regarding information security, and thus foster an environment where users are more likely to enact problem-focused actions in response to a perceived threat.

This is a complex proposition, as it moves beyond the technical aspects of security control and into the organizational dynamics and culture. Access restrictions are a necessary part of working in a secure environment, with a fine balance between these necessary restrictions, and what may be perceived by users as a hindrance to their role. Interestingly, Ruighaver et al. (2007) found that employees in high security organizations are more accepting of the limitations and controls on their systems due to the accompanying security culture. This presents an interesting practical dimension – that through appropriate framing and culture, users may have a more positive perception of security controls, even when faced with increased restriction.

In the context of our work, this suggests that it may indeed be possible to shift users from an emotion-focused response toward a problem-focused behavioral pathway by strengthening the orientation and motivation towards security at a cultural level. Advancements in organizational information security are often accompanied by increased technical capacity and automation in the security workflow. However, we argue that technical controls are still only one tool at the security manager's disposal. A broader organizational implication is that rather than further diminishing the user's (perception of) control, users may be invited to take a more active role in the identification and response to information security threats. Folkman and Moskowitz (2004) highlighted that PFC strategies are more effective when users feel in a position to do something about the demand. Conversely, if users do not possess the agency to address the stressor, then they may favor EFC mechanisms. Thus, a work environment that is characterized by higher autonomy may potentially yield better results in terms of security behaviors.

7. Conclusion

Though much is known about the determinants of user information security behavior, many questions remain as to why users often respond minimally or even appear to not respond at all to an otherwise obvious security threat. In this study, we examine this issue by considering the role of EFC responses in the context of information security. Prior work has almost exclusively focused on users' security behaviors which include problem-focused responses. However, users may also undertake a range of internal self-regulation processes which may not be apparent to the observer. These responses, known as EFC, may include avoiding stressful situations, or convincing oneself that the threat is less severe than in reality. In this study, we considered threat devaluation as a form of EFC and demonstrated that many determinants of security behavior also influence users to devalue the threat. This has the impact of relieving their stress but may delay the enactment of any practical security behavior. This is a promising area for future research as prior work has largely been limited to PFC. Thorough consideration of both problem-focused as well as emotion-focused user responses holds promise to yield greatly improved models of information security behavior and to ultimately benefit researchers, practitioners, and end users alike.

CRediT authorship contribution statement

Nik Thompson: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Supervision, Validation, Writing – original draft, Writing – review & editing. **Tanya McGill:** Conceptualization, Formal analysis, Investigation, Methodology, Project administration, Validation, Writing – original draft, Writing – review & editing. **Nidhi Narula:** Data curation, Investigation, Validation, Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Appendix

Table A.1
Measurement items and sources.

Item	SouSource
Perceived severity	
Having my credentials stolen would be a serious problem for me	Woon et al. (2005)
Loss of information resulting from a phishing attack would be a serious problem for me	Woon et al. (2005)
Having my confidential information stolen by someone without my consent or knowledge would be very problematic for me	Workman et al. (2008)
I view information security attacks on me as harmful	Workman et al. (2008)
I believe that protecting my sensitive information is important	Workman et al. (2008)
Perceived vulnerability	
I could be subject to a serious information theft	Woon et al. (2005)
I feel that I could be vulnerable to an information theft or a malware attack resulting from clicking on a link received in email	Thompson et al. (2017)
It is likely that my private information will be compromised in the future	Thompson et al. (2017)
My information and data are vulnerable to security breaches	Thompson et al. (2017)
Response costs	
Taking security measures inconveniences me *	Thompson et al. (2017)
There are too many overheads associated with taking security measures to protect from email phishing attacks	Woon et al. (2005)
Taking security measures would require considerable investment of effort	Woon et al. (2005)
Implementing security measures on my device would be time consuming	Woon et al. (2005)

(*continued on next page*)

Table A.1 (*continued*)

Item	SouSource
The cost of implementing recommended security measures exceeds the benefits	Workman et al. (2008)
The impact of security measures on my productivity exceeds the benefits *	Thompson et al. (2017)
Response efficacy	
Enabling security measures on my device will prevent security breaches	Woon et al. (2005)
Implementing security measures on my device is an effective way to prevent hackers	Woon et al. (2005)
Enabling security measures on my device will prevent hackers from stealing my identity	Woon et al. (2005)
The preventative measures available to stop people from getting confidential personal or financial information on my device are effective	Thompson et al. (2017)
Self-efficacy	
I feel comfortable taking measures to secure my sensitive Information	Anderson and Agarwal (2010)
Taking the necessary security measures is entirely under my control.	Anderson and Agarwal (2010)
I have the knowledge to differentiate phishing emails from legitimate ones	Anderson and Agarwal (2010)
Taking the necessary security measures is easy for me	Anderson and Agarwal (2010)
I can protect my information by myself *	Anderson and Agarwal (2010)
Fear	
I am scared to enter my details in online forms and links received via email.	Adapted from Masuch et al. (2021)
I only open emails from people I know	Adapted from Masuch et al. (2021)
I fear receiving malware in an email	Adapted from Masuch et al. (2021)
I look at email scams in the news and feel fearful about the impact if it was to happen to me.	Adapted from Masuch et al. (2021)
It scares me to think that if I open a malicious email, it could lead to a lot of destruction	Adapted from Masuch et al. (2021)
PFC behavior	
I make every effort to scan the email thoroughly before I click on any links	Wang et al. (2017)
I concentrate hard on every email trying to analyse for phishing indicators	Wang et al. (2017)
I try to concentrate on the task while opening emails	Wang et al. (2017)
Threat devaluation	
Phishing threats are not worth getting upset about	Davey (1993)
I can put up with phishing threats as long as everything else is OK in life	Davey (1993)
There’s nothing else I can do, so there is no point worrying	Davey (1993)
Phishing threats are not worth worrying about	Davey (1993)
I don’t take phishing threats too seriously	Davey (1993)

* Item removed during measurement model assessment.

Table A.2
Fornell-Larker criterion results.

	Fear	Perceived severity	Perceived vulnerability	PFC behavior	Response cost	Response efficacy	Self-efficacy	Threat devaluation
Fear	**0.71**							
Perceived severity	0.42	**0.79**						
Perceived vulnerability	0.36	0.35	**0.71**					
PFC behavior	0.49	0.49	0.26	**0.77**				
Response cost	−0.02	−0.11	0.10	−0.12	**0.70**			
Response efficacy	0.45	0.50	0.35	0.49	−0.05	**0.72**		
Self-efficacy	0.38	0.48	0.24	0.49	−0.14	0.58	**0.71**	
Threat devaluation	−0.31	−0.35	−0.17	−0.22	0.43	−0.22	−0.14	**0.72**

Table A.3
HTMT results.

	Fear	Perceived severity	Perceived vulnerability	PFC behavior	Response cost	Response efficacy	Self-Efficacy
Fear							
Perceived severity	0.55						
Perceived vulnerability	0.52	0.43					
PFC behavior	0.74	0.66	0.37				
Response cost	0.02	0.14	0.16	0.18			
Response efficacy	0.67	0.65	0.49	0.71	0.08		
Self-efficacy	0.54	0.62	0.33	0.72	0.21	0.83	
Threat devaluation	0.43	0.42	0.20	0.30	0.59	0.30	0.17

References

Abbasi, A., Zahedi, F.M., Chen, Y., 2016. Phishing susceptibility: the good, the bad, and the ugly. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 169–174.

Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Q. 34 (3), 613–643. https://doi.org/10.2307/25750694.

Anti-Phishing Working Group, 2022. Phishing Activity Trends Report: 2nd Quarter 2022 from. https://apwg.org/trendsreports/.

Arachchilage, N.A.G., Love, S., 2013. A game design framework for avoiding phishing attacks. Comput. Human Behav. 29, 706–714.

Arachchilage, N.A.G., Love, S., Beznosov, K., 2016. Phishing threat avoidance behaviour: an empirical investigation. Comput. Human Behav. 60, 185–197. https://doi.org/10.1016/j.chb.2016.02.065.

Bax, S., McGill, T., Hobbs, V., 2021. Maladaptive behaviour in response to email phishing threats: the roles of rewards and response costs. Comput. Secur. 106, 102278 https://doi.org/10.1016/j.cose.2021.102278.

Belanger, F., Crossler, R.E., 2019. Dealing with digital traces: understanding protective behaviors on mobile devices. J. Strat. Inf. Syst. 28 (1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., Cotten, S., 2015. Determinants of online safety behaviour: towards an intervention strategy for college students. Behav. Inf. Technol. 34 (10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448.

Boss, S., Galletta, D., Lowry, P., Moody, G., Polak, P., 2015. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 39, 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5.

Carver, C.S., Scheier, M.F., Weintraub, J.K., 1989. Assessing coping strategies: a theoretically based approach. J. Pers. Soc. Psychol. 56 (2), 267–283.

Chen, D.Q., Liang, H., 2019. Wishful thinking and IT threat avoidance: an extension to the technology threat avoidance theory. IEEE Trans. Eng. Manage 66 (4), 552–567. https://doi.org/10.1109/TEM.2018.2835461.

Chen, Y., Galletta, D., Lowry, P., Luo, R., Moody, G., 2021. Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. Inf. Syst. Res. 32 (3), 1043–1065. https://doi.org/10.1287/isre.2021.1014.

Chen, Y., Luo, X., Li, H., 2022. Beyond adaptive security coping behaviors: theory and empirical evidence. Inf. Manage. 59 (2), 103575 https://doi.org/10.1016/j.im.2021.103575.

Chen, Y., Zahedi, F., 2016. Individuals' Internet security perceptions and behaviors: polycontextual contrasts between the United States and China. MIS Q. 40 (1), 205–222.

Chenoweth, T., Minch, R., Gattiker, T., 2009. Application of protection motivation theory to adoption of protective technologies. In: 42nd Hawaii International Conference on System Sciences. Hawaii. IEEE.

Cho, H., Li, P., Goh, Z., 2020. Privacy risks, emotions, and social media. ACM Trans. Comput.-Human Interact. (TOCHI) 27, 1–28.

Compas, B.E., Connor-Smith, J.K., Saltzman, H., Thomsen, A.H., Wadsworth, M.E., 2001. Coping with stress during childhood and adolescence: problems, progress, and potential in theory and research. Psychol. Bull. 127, 87–127. https://doi.org/10.1037/0033-2909.127.1.87.

D'Arcy, J., Herath, T., Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. J. Manage. Inf. Syst. 31 (2), 285–318.

Davey, G.C.L., 1993. A comparison of three cognitive appraisal strategies: the role of threat devaluation in problem-focussed coping. Pers. Individ. Dif. 14 (4), 535–546. https://doi.org/10.1016/0191-8869(93)90146-T.

Dewe, P.J., O'Driscoll, M.P., Cooper, C., 2010. Coping with Work Stress: A Review and Critique. Wiley-Blackwell, Chichester, UK.

Folkman, S., 1988. Ways of Coping Questionnaire, Sampler Set, Manual, Test Booklet, Scoring Key. Consulting Psychologists Press, Palo Alto, CA [1988]©1988.

Folkman, S., Lazarus, R.S., Gruen, R.J., DeLongis, A., 1986. Appraisal, coping, health status, and psychological symptoms. J. Pers. Soc. Psychol. 50 (3), 571–579.

Folkman, S., Moskowitz, J.T., 2004. Coping: pitfalls and promise. Annu. Rev. Psychol. 55, 745–774.

Hair, J., Sarstedt, M., Ringle, C., Hult, G.T., 2017. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed. Sage, Los Angeles.

Henseler, J., Ringle, C.M., Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Market. Sci. 43 (1), 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Jansen, J., van Schaik, P., 2018. Persuading end users to act cautiously online: a fear appeals study on phishing. Inf. Comput. Secur. 26 (3), 264–276. https://doi.org/10.1108/ICS-03-2018-0038.

Jordan, P.J., Troth, A.C., 2020. Common method bias in applied settings: the dilemma of researching in organizations. Aust. J. Manage. 45 (1), 3–14. https://doi.org/10.1177/0312896219871976.

Lazarus, R.S., 1996. The role of coping in the emotions and how coping changes over the life course. In: Maletesta-Magni, C., McFadden, S.H. (Eds.), Handbook of Emotion, Adult Development, and Aging. Academic Press, New York, pp. 289–306.

Lazarus, R.S., Folkman, S., 1984. Stress, Appraisal, and Coping. Springer, New York.

Leventhal, H., 1970. Findings and theory in the study of fear communications. Adv. Exp. Soc. Psychol. 5, 119–186. https://doi.org/10.1016/S0065-2601(08)60091-X.

Leventhal, H., 1971. Fear appeals and persuasion: the differentiation of a motivational construct. Am. J. Public Health 61 (6), 1208–1224.

Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS Q. 33 (1), 71–90. https://doi.org/10.2307/20650279.

Liang, H., Xue, Y., 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. 11 (7), 394–413.

Liang, H., Xue, Y., Pinsonneault, A., Wu, Y.A., 2019. What users do besides problem-focused coping when facing IT security threats: an emotion-focused coping perspective. MIS Q. 43 (2), 373–394.

Lindell, M.K., Whitney, D.J., 2001. Accounting for common method variance in cross-sectional research designs. J. Appl. Psychol. 86 (1), 114–121. https://doi.org/10.1037/0021-9010.86.1.114.

Lowry, P.B., Gaskin, J., 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it. IEEE Trans. Prof. Commun. 57 (2), 123–146.

Marett, K., McNab, A.L., Harris, R.B., 2011. Social networking websites and posting personal information: an evaluation of protection motivation theory. AIS Trans. Hum.-Comput. Interact. 3 (3), 170–188.

Masuch, K., Hengstler, S., Schulze, L., & Trang, S. (2021). *The impact of threat and efficacy on information security behavior: applying an extended parallel process model to the fear of Ransomware*.

Miller, C.T., Kaiser, C.R., 2001. A theoretical perspective on coping with stigma. J. Soc. Issues 57 (1), 73–92.

Mills, A.M., Sahai, N., 2019. An empirical study of home user intentions towards computer security. In: Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 4834–4840.

Moody, G., Siponen, M., Pahnila, S., 2018. Toward a unified model of information security policy compliance. MIS Q. 42 (1), 285–311. https://doi.org/10.25300/MISQ/2018/13853.

Mou, J., Cohen, J.F., Bhattacherjee, A., Kim, J., 2022. A test of protection motivation theory in the information security literature: a meta-analytic structural equation modeling approach. J. Assoc. Inf. Syst. 23 (1), 196–236. https://doi.org/10.17705/1jais.00723.

Mwagwabi, F., McGill, T., Dixon, M., 2018. Short-term and long-term effects of fear appeals in improving compliance with password guidelines. Commun. Assoc. Inf. Syst. 42, 147–182.

Pearlin, L.I., Schooler, C., 1978. The structure of coping. J. Health Soc. Behav. 19 (1), 2–21.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879–903.

Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of method bias in social science research and recommendations on how to control it. Annu. Rev. Psychol. 63 (1), 539–569. https://doi.org/10.1146/annurev-psych-120710-100452.

Ringle, C.M., Wende, S., Will, A., 2005. Smart PLS 2.0 M3. University of Hamburg, Hamburg. Retrieved from. www.smartpls.de.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91 (1), 93–114.

Rogers, R.W, 1983. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo, B.L., Petty, L.L. (Eds.), Social Psychophysiology: A Source Book. Guildford Press, London, pp. 153–176.

Ruighaver, A.B., Maynard, S.B., Chang, S., 2007. Organisational security culture: extending the end-user perspective. Comput. Secur. 26 (1), 56–62.

Shahbaznezhad, H., Kolini, F., Rashidirad, M., 2020. Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter? J. Comput. Inf. Syst. 61 (6), 539–550. https://doi.org/10.1080/08874417.2020.1812134.

Skinner, E.A., Edge, K., Altman, J., Sherwood, H., 2003. Searching for the structure of coping: a review and critique of category systems for classifying ways of coping. Psychol. Bull. 129, 216–269. https://doi.org/10.1037/0033-2909.129.2.216.

Thompson, N., McGill, T., Wang, X., 2017. Security begins at home": determinants of home computer and mobile device security behavior. Comput. Secur. 70, 376–391. https://doi.org/10.1016/j.cose.2017.07.003.

Tourangeau, R., Rips, L.J., Rasinski, K., 2000. The Psychology of Survey Response. Cambridge University Press, Cambridge, UK.

Verkijika, S.F., 2019. If you know what to do, will you take action to avoid mobile phishing attacks": self-efficacy, anticipated regret, and gender. Comput. Human Behav. 101, 286–296. https://doi.org/10.1016/j.chb.2019.07.034.

Wang, J., Li, Y., Rao, H.R., 2017. Coping responses in phishing detection: an investigation of antecedents and consequences. Inf. Syst. Res. 28 (2), 378–396.

Warkentin, M., Johnston, A.C., Shropshire, J., Barnett, W.D., 2016. Continuance of protective security behavior: a longitudinal study. Decis. Support. Syst. 92, 25–35. https://doi.org/10.1016/j.dss.2016.09.013.

Williams, E.J., Joinson, A.N., 2020. Developing a measure of information seeking about phishing. J. Cybersecur. 6 (1), 1–16. https://doi.org/10.1093/cybsec/tyaa001.

Witte, K., 1992. Putting the fear back into fear appeals: the extended parallel process model. Commun. Monogr. 59 (4), 329–349. https://doi.org/10.1080/03637759209376276.

Witte, K., 1994. Fear control and danger control: a test of the extended parallel process model (EPPM). Commun. Monogr. 61 (2), 113–134. https://doi.org/10.1080/03637759409376328.

Woon, I., Tan, G., Low, R.T., 2005. A protection motivation theory approach to home wireless security. In: Proceedings of the Twenty-Sixth International Conference on Information Systems, pp. 367–380.

Workman, M., Bommer, W.H., Straub, D., 2008. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Human. Behav. 24, 2799–2816.

Xin, T., Siponen, M., Chen, S., 2021. Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats. Behav. Inf. Technol. 41 (13), 2835–2859.

Nik Thompson is an Associate Professor of Information Systems at Curtin University, Australia. He holds MSc and PhD degrees and works in the area of Computer Security and Information Systems. His research interests include privacy, human-computer interaction and information security. His work has appeared in leading journals including Journal of the Association for Information Science and Technology, Computers & Security and Behavior & Information Technology. For more information, please visit https://www.nikthompson.com

Tanya McGill is an Adjunct Research Fellow at Curtin University in Western Australia. Her major research interests include information privacy and security, technology adoption and e-learning. Her work has appeared in various journals including *Computers in Human Behavior, Computers & Security, Computers & Education, Decision Support Systems, Behaviour and Information Technology*, and *International Journal of Human-Computer Studies.*

Nidhi Narula is a cyber security professional based at Western Power in Perth, Western Australia. She holds a master's degree in information systems from Curtin University, with research experience specializing in human-centred design and information systems. She combines her educational background and her role at Western Power with a deep fascination for understanding people's needs and motivations. She actively engages in hypothesis-driven design and development to gain insights at the intersection of technology and human behaviour. She aims to uncover sustainable technological solutions that generate continual value by fostering positive experiences and meaningful connections.