Computers & Security 165 (2026) 104872

Contents lists available at ScienceDirect

Computers & Security

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

Full Length Article

"Not all bad": Determinants and impacts of emotion-focused and problem-focused coping in information security behavior

Tanya McGill, Nik Thompson *, Nidhi Narula

Curtin University, Perth, Australia

ARTICLE INFO

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

ABSTRACT

Users may respond to threats with a wide range of coping strategies in addition to protective information security behavior. However, relatively little is known about emotion-focused coping (EFC), and prior work has often considered such responses to be "maladaptive." We examine EFC in the context of phishing and demonstrate that it can, in fact, have a positive influence on security behavior. Our research model builds on the established foundation of protection motivation theory and incorporates threat devaluation and positive reappraisal as forms of EFC. We collected quantitative data from 518 respondents and tested our model with PLS structural equation modeling to provide empirical insights into how threat and coping appraisals can lead to both emotion-focused and problem-focused responses. We find that EFC responses are nuanced and thus classify them according to whether the individual response is to either approach or avoid the threat. As these coping responses may be shaped by user perceptions, our findings provide opportunities to both protect users and develop a more comprehensive understanding of information security behavior.

1. Introduction

As meta-analyses such as those by Mou et al. (2022) and Sutton and Tompson (2025) demonstrate, a large amount of behavioral information security research has explored factors that may influence whether and how technology users protect themselves against information security. Theories such as Protection Motivation Theory (PMT) (Rogers, 1975) and Technology Threat Avoidance Theory (TTAT) (Liang and Xue, 2009) underpin much of this work. This research has led to valuable insights and contributed to approaches to improving security behavior, but users still do not consistently adopt protection behaviors. Furthermore, when a user faces an information security threat, they might not focus their effort on protection behaviors, known as problem-focused coping (PFC) responses; for example, using anti-phishing software tools. Instead, they might manage the emotional impact the threat causes through emotion-focused coping (EFC) (Chen et al., 2022; Thompson et al., 2024; Xin et al., 2021). For example, wishing that nothing negative will happen if they open a phishing email (wishful thinking), denying that identity theft resulting from phishing could happen to them (denial), and underestimating the impact of a phishing attack (threat devaluation).

Haag et al. (2021) have called for more research to help understand users' EFC responses, including identifying the distinct types of these responses and determining what factors influence them. Recent research (Thompson et al., 2024) has shown that threat devaluation, where users respond to phishing threats by devaluing them in order to reduce their stress, is a form of EFC that plays a role in their responses to phishing threats. This study also found that many determinants of security behavior influence users to devalue the threat. Using threat devaluation as a response has the impact of relieving stress but may delay the enactment of practical information security behavior. Another EFC response that has been studied in the health domain, but not the information security context, is positive reappraisal. Positive reappraisal is a coping response where threats are reconstrued as having a potentially positive benefit, so that the individual appraises the threat as a challenge, enabling them to ultimately adopt problem-focused responses (Davey, 1993). As the role of positive reappraisal in coping with security threats has not yet been studied, and very little is known about threat devaluation, this research extends the work of Liang et al. (2019) and Thompson et al. (2024), which consider the roles of different types of EFC in phishing protection behavior. This study proposes and tests a model that includes the roles that positive reappraisal and threat devaluation play in how users respond to information security threats. Phishing was used as the context for this research as phishing is an

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

https://doi.org/10.1016/j.cose.2026.104872
Received 20 August 2025; Received in revised form 4 November 2025; Accepted 23 February 2026
Available online 26 February 2026

increasingly concerning information security threat, with the Anti-Phishing Working Group (2024) reporting the detection of over 300,000 unique phishing websites per month.

The study addresses two main research questions:

RQ1: How are positive reappraisal and threat devaluation influenced by factors that have been found to influence phishing protection behavior?
RQ2: How do positive reappraisal and threat devaluation influence phishing protection behavior?

Previous information security research has demonstrated that there can be gender differences in both privacy and security behavior and the perceptions that influence these behaviors (McGill and Thompson, 2021). Little is known about how gender might influence the use of EFC responses in response to phishing threats, but Liang et al. (2019) found that gender influenced an EFC construct that included emotional support seeking and venting, with females more likely to employ these EFC responses, but not others. Given this finding, our study also extends the work of Liang et al. (2019) by exploring whether gender plays a role in the use of positive reappraisal and threat devaluation:

RQ3: Does gender play a role in the use of positive reappraisal and threat devaluation in response to phishing threats?

2. Literature review

The psychological theory of stress and coping (Lazarus, 1966) describes how individuals respond to environmental threats or challenges through processes of cognitive appraisal and coping. Cognitive appraisal is the initial environmental assessment made by the individual, by which they ascertain if there is a potential threat, as well as if anything can be done in response to the threat. The evaluation of potential harm and potential responses are commonly described as primary and secondary appraisal processes, though they may occur in parallel (Lazarus and Folkman, 1984). Primary and secondary appraisals both lead to a determination of whether the perceived threat is significant and in what way (e.g. is it harmful or challenging).

Coping can be 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). Thus, environmental conditions that are perceived as threats via the appraisal processes described above will invoke a coping response. Coping is recognized to have two major functions: regulating the stressful experience (EFC) and taking action to address the source of the threat or distress (PFC). Thus, when faced with an information security related threat, it is possible that the effort a user exerts toward managing the situation need not be directly problem-focused but may instead be inwardly focused on managing the associated emotional impact of the threat. User responses to security threats may thus be categorized into EFC and PFC.

Foundational work on coping discussed a broad range of approaches that people may use to react to stressful environmental conditions or threats. For example, they might directly address the threat to "*come up with a couple of different solutions to the problem*", or they might "*be inspired*" by the situation (Folkman and Lazarus, 1980). These coping responses have subsequently been shown to fit distinctly into problem or emotion-focused domains (e.g. Tobin et al., 1989). Within the class of EFC responses, several of these identified coping responses have been 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).

Though a large number of coping strategies have been identified (Skinner et al., 2003), there is no broad consensus on the structure of coping within the two higher-order dimensions of EFC and PFC. Simply organizing coping strategies into problem-focused or emotion-focused mechanisms, though convenient and easily understood, says little about the implications of a particular coping style for the individual when faced with a stressor. This limitation has been addressed by Scheier et al. (1986), who considered how the strategies guide the individual to address the problem. They conclude that while PFC strategies may be correlated with one another, some EFC strategies may serve a range of functions, some of which address a stressor (i.e. approach it) while others may avoid it. This more functional classification is compatible with early work (Freud, 1915), which suggests that coping strategies exist within two different high-level dimensions - those which either *approach* or *avoid* a stressor. Thus, the approach/avoidance dimensions provide a suitable framework within which we examine the different coping mechanisms in this research.

Examples of approach coping could include strategies such as taking a specific action (i.e. PFC), planning, or positive reappraisal of the situation (Freire et al., 2020). Avoidance or evasive strategies, on the other hand, are those coping mechanisms in which the stressful situation is not directly addressed. These might include denial or wishful thinking. There is some evidence that approach coping responses are generally related to positive outcomes, while this is not the case for avoidance strategies. For example, information security studies have shown that the emotion-focused responses of denial (Xin et al., 2021) and wishful thinking (Liang et al., 2019) can be regarded as potentially counterproductive, as they can hinder adoption of PFC responses whereas *approach* 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).

Haag et al. (2021) called for more research to help understand users' EFC responses to security threats, and recent studies have started to answer this call by studying 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).

2.1. Positive reappraisal

Positive reappraisal describes efforts to recast an otherwise negative situation in terms of personal growth (Folkman et al., 1986). By reinterpreting the situation in positive terms, the individual may believe that something can be gained from the situation (Folkman and Moskowitz, 2000). This is consistent with the definition of an EFC response, as it attends to the internal emotional state of the individual without directly addressing the reality of the situation. It is worth noting that the goal is not to distort the reality of the situation itself, but to recognize the potential for a positive experience (Nowlan et al., 2015). Positive reappraisal would therefore be considered an approach response as it involves addressing the stressor.

Interestingly, prior work has found a high correlation between positive reappraisal and problem-focused forms of coping (Folkman and Lazarus, 1985). This also suggests that although positive reappraisal is an emotion-focused response, it may encourage PFC behaviors. Prior work on this element of coping has measured positive reappraisal through a variety of measures and in different environments (Nowlan et al., 2015); however, it has not previously been studied in the context of information security behavior. As positive reappraisal may be a determinant of practical security behavior (i.e. PFC), understanding its role in security threat appraisal and response has the potential to be impactful in protecting users against phishing threats.

2.2. Threat devaluation

Threat devaluation is an EFC strategy where someone acknowledges a problem or threat but tries to lessen its stressful impact. For instance, in cybersecurity, a user might know about email phishing but downplay the risk, feeling no urgent need to act. Unlike denial, threat devaluation means the threat isn't ignored, but immediate action isn't seen as necessary.

Research by Davey (1993) in a health context suggests that threat devaluation can be linked to PFC when people deal with manageable threats. Adopting this approach to lessen the stress of lower-impact threats can potentially allow individuals to save their focus for more serious issues.

Understanding threat devaluation is crucial for information security because different types of EFC can affect PFC. If threat devaluation operates as an approach EFC response (such as seeking social support), it could potentially help PFC. However, if it is more like avoidance EFC (e.g. denial), it might hinder PFC. By understanding threat devaluation and its influencing factors, security professionals can better grasp users' emotional states and help them manage security threats through direct support, training, and awareness campaigns.

2.3. Coping models and information security threats

PMT explains how individuals are motivated to respond to potential threats based on their appraisals of both the threat and the available coping mechanisms (Rogers, 1975, 1983). Originally developed as a way to understand health-related behaviors, PMT is now one of the most commonly applied theories in behavioral information security research (Haag et al., 2021; Hassandoust et al., 2020), a key area of the information security field (Boss et al., 2015).

Over time, PMT has been used as the basis to study the potential role of new constructs such as descriptive norm (Thompson et al., 2017) and information security culture (Alrawhani et al., 2025). However, much of this prior work has only considered PFC (in the form of security intentions or behaviors) as the outcome variable of interest. Given that a wide range of alternative coping responses exist that are not problem-focused, there is potential for impactful findings into why end users often fail to enact security measures or comply with organizational directives. The initial research on this has largely used PMT (e.g., Xin et al., 2021), TTAT (e.g., Chen and Liang, 2019), and Witte's (1992) Extended Parallel Process Model (EPPM) (e.g., Chen et al., 2022; Masuch et al., 2021) to help understand the part that EFC responses play in how users respond to information security threats. However, apart from Liang et al. (2019), the EFC responses investigated have largely been avoidance strategies, and no previous research has investigated the role of positive appraisal in the information security domain. In this study, we build on previous research using PMT and EPPM to explore the roles of two little-studied dimensions of EFC: positive reappraisal and threat devaluation. These are relatively independent constructs with distinctive qualities contributing separately to the prediction of coping subscale scores – i.e. types of coping (Davey, 1993). The development of the research model and hypotheses are explained in more detail in Section 3.

2.4. Gender and coping with information security threats

To better understand how positive reappraisal and threat devaluation influence phishing protection behavior, this study also explores whether gender plays a role. Previous research has highlighted gender differences in security behaviors and in perceptions that can influence information security intentions and behaviors (Gratian et al., 2018; Jagatic et al., 2007; McGill and Thompson, 2021; Sheng et al., 2010). For example, McGill and Thompson (2021) identified gender differences in over 40 % of the security and privacy behaviors they investigated, concluding that overall levels of both were significantly lower for females than males. The differences tended to be with those behaviors that require more technical skill, such as enabling a firewall on a home network and installing security software. This was despite females having higher levels of perceived threat severity and descriptive norm. Several studies have also found that females have a greater vulnerability to phishing attacks (Jagatic et al., 2007; Sheng et al., 2010), with Sheng et al. (2010) finding that female users were more likely to click on links in phishing emails and proceed to provide personal information. Both McGill and Thompson (2021) and Sheng et al. (2010) also reported that female users had less security knowledge and training than males, suggesting it as part of the reason for the differences in susceptibility to threats because of reduced ability to protect against them.

Very little research has explored the potential role of gender in EFC. However, in the context of decision making, Flores-Torres et al. (2022) found that while positive reappraisal reduced negative emotions for both men and women, it improved women's decision making in a widely used decision making test (Iowa Gambling Test; Bechara et al., 1994) yet impaired men's. This was despite men in the control group having better decision-making performance on average than females. They suggested that males may be able to more rapidly direct their cognitive resources to PFC than females, and in doing so, not deal with the negative emotion. In contrast, when they do employ positive reappraisal, it may negatively affect their decision-making because their cognitive resources are split between regulation of their emotions and the task, something that did not occur with females.

In the information security domain, Chen et al. (2022) found that gender did not influence the use of defensive-avoidance, but did influence whether users sought help, with females more likely to do so. Similarly, neither Marett et al. (2011) nor Xin et al. (2021) found significant gender differences in levels of avoidance EFC responses. In Marett et al. (2011), defensive-avoidance and hopelessness were considered, and in Xin et al. (2021), five types of avoidance EFC responses were tested (defensive-avoidance, reactance, hopelessness, wishful thinking, and fatalism).

In the only study to date that has considered approach EFC responses, Liang et al. (2019) found that although gender did not influence their avoidance EFC construct (called inward EFC and which included denial, distancing and wishful thinking) it had a small positive influence on their approach EFC construct (called outward EFC, with emotional support seeking and venting included), with females more likely to use approach strategies. Given this research suggesting that gender may be important in the adoption of approach EFC responses to security threats, this study also explores whether gender plays a role in the use of positive reappraisal and threat devaluation.

3. Model development

Roger's PMT (1975, 1983) and Witte's EPPM (1992) provide frameworks for understanding how individuals react to perceived threats. They include elements that represent whether individuals engage in danger control, aimed at mitigating the threat, or fear control, focused on managing their emotional response. EPPM has a more explicit focus on EFC, but does not accommodate the co-existence of EFC and PFC (van 't Riet and Ruiter, 2013). We draw on both PMT and EPPM to explore how threat devaluation and positive reappraisal impact responses to phishing threats and propose the model depicted in Fig. 1, with construct definitions provided in Table 1.

Both PMT (Rogers, 1983) and EPPM (Witte, 1994) emphasize that perceived severity and vulnerability drive fear. These relationships, where heightened perceptions of threat are associated with increased fear, have been consistently observed across various information security contexts (Mou et al., 2022), including phishing. Specifically, research demonstrates that when individuals perceive the threat from phishing emails as more severe or themselves as more vulnerable to the threat, the fear emotion intensifies (Arachchilage and Love, 2013; Bax et al., 2021; Jansen and van Schaik, 2018; Thompson et al., 2024). 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 revised PMT (Rogers, 1983) and to the EPPM (Witte, 1994), which propose that when fear is invoked, the user takes action to resolve the fear. In information security research, this action

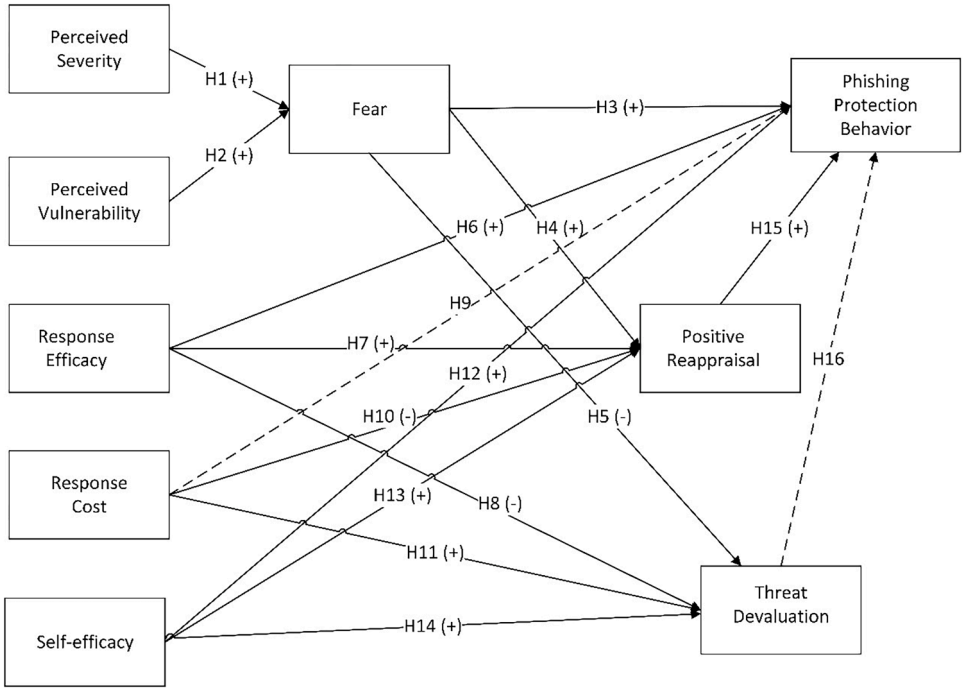

Fig. 1. Research model.

Table 1
Definitions of the constructs.

Construct	Definition
Perceived severity	An individual's perception of the seriousness of the consequences of falling victim to a phishing threat.
Perceived vulnerability	An individual's perception of the likelihood of falling victim to a phishing threat.
Fear	An emotional response to a perceived threat, in this case, phishing.
Response efficacy	The extent to which an individual believes that the recommended actions will effectively mitigate or eliminate the phishing threat.
Self-efficacy	An individual's beliefs about how successfully they will be able to perform protective behaviors to avoid falling victim to a phishing attack.
Response cost	The perceived opportunity cost that an individual believes is associated with taking protective action against phishing threats (e.g. time, effort, or financial).
Phishing protection behavior	Problem-focused responses to a threat that occur when an individual undertakes protective behavior to deal directly with a phishing threat to protect themselves from the possible damage.
Positive reappraisal	An EFC response that involves an optimistic outlook and viewing a phishing incident as a learning experience or as allowing for the potential for growth (Hakim-Larson et al., 1999).
Threat devaluation	An EFC response where the threat is recognized but 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.

has generally been considered to be problem-focused, and previous studies provide support for the impact of fear on security behavior (e.g., Boss et al., 2015; Chen et al., 2022; Liang et al., 2019; Mwagwabi et al., 2018), including with phishing threats (Arachchilage and Love, 2013; Bax et al., 2021; Thompson et al., 2024). Hence, we hypothesize that:

H3: Fear positively influences phishing protection behavior.

However, more recent research has highlighted that emotions can play a role in whether and how users take these actions. Liang et al. (2019) argue that fear has a positive influence on a range of EFC responses, and several studies have found that fear associated with security threats influences the levels of EFC responses. Fear has also been shown to increase avoidance and disengagement (Cho et al., 2020) and denial, wishful thinking, venting, and seeking social support (Liang et al., 2019). Despite the finding from Thompson et al. (2024) that fear had a negative influence on threat devaluation, it seems likely that increases in fear will lead to increases in positive appraisal in response to security threats. That is, users who experience higher levels of fear in response to phishing threats may experience increased levels of positive appraisal of the situation (e.g. considering that they will learn from the threat), and thereby emotionally cope with it. Therefore, an increase in an individual's level of fear about email phishing threats should increase their positive reappraisal of the threat situation, and the following is hypothesized:

H4: Fear positively influences positive reappraisal.

Although several studies have found that fear associated with security threats positively influences the levels of EFC responses (Cho et al., 2020; Liang et al., 2019), Thompson et al. (2024) argued that increases in fear should be associated with decreases in threat devaluation. This argument was made based on the findings of Davey (1993) about differences in responses to threats depending on whether the individual perceives the threat as controllable. In the phishing context, users can regard phishing as a potentially controllable threat (Abbasi et al., 2016; Verkijika, 2019); they may therefore 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. The results of Thompson et al. (2024) supported the proposition. Therefore, we hypothesize that:

H5: Fear negatively influences threat devaluation.

The results of previous information security studies have demonstrated that increases in perceptions of response efficacy are associated with increased protective behavior, including when the threat relates to

phishing (Arachchilage and Love, 2013; Bax et al., 2021; Shahbaznezhad et al., 2020; Thompson et al., 2024; Williams and Joinson, 2020); therefore, we hypothesize:

H6: Response efficacy positively influences phishing protection behavior.

Although the perceived efficacy of potential responses to information security threats has been shown to influence users' protective behavior in response to some kinds of security threats, less is known about how response efficacy and other aspects of coping appraisal influence EFC. Xin et al. (2021) proposed that response efficacy would have a negative influence on several avoidance types of EFC (defensive-avoidance, reactance, wishful thinking, hopelessness, and fatalism) and found that this was the case for most of the EFC responses they included in the study. The influence of response efficacy on approach EFC has not yet been studied, but we argue that users who believe that the recommended actions (e.g. using anti-phishing toolbars in browsers and anti-phishing software) will effectively mitigate or eliminate phishing threats are more likely to experience positive reappraisal of the threat. That is, they see a phishing threat as a learning experience, enabling them to protect their data better in the future. Therefore, we hypothesize:

H7: Response efficacy positively influences positive reappraisal.

As mentioned above, Xin et al. (2021) found that all the types of EFC they studied, except defensive-avoidance, were negatively influenced by increases in response efficacy. Consistent with this, in the phishing context, Thompson et al. (2024) found that response efficacy also had a negative influence on threat devaluation; that is, the more that users believed that responses to the phishing threats were effective, the less they used threat devaluation as a response. Therefore, we hypothesize:

H8: Response efficacy negatively influences threat devaluation.

The revised PMT (Rogers, 1983) includes response cost as a negative influence on intention to perform protective behavior. However, the results of information security research on this relationship have been mixed, and the meta-analysis by Mou et al. (2022) found no support for the role of response cost. Similarly, in the phishing protection context, while Arachchilage and Love (2013) and Bax et al. (2021) found response cost to play a role, given the conclusion drawn by Mou et al. (2022) and the fact that neither Jansen and van Schaik (2018) nor Thompson et al. (2024) found that perceived response cost influenced the whether users protected themselves against phishing threats, we hypothesize that:

H9: Response cost does not influence phishing protection behavior.

The role of response cost in influencing EFC responses is not yet well understood. Two previous information security studies found that response cost had a positive influence on avoidance EFC responses (Chenoweth et al., 2009; Marett et al., 2011); that is, the higher the perceived cost of the response, the more likely users were to respond in a potentially counterproductive way that addressed their emotions but did not deal directly with the threat. Positive reappraisal is, however, an approach form of EFC that involves viewing the threat as a learning experience that can provide potential for growth (Davey, 1993; Folkman and Lazarus, 1985). We therefore argue that higher perceptions of the cost of responding to phishing threats will result in users being less likely to engage in positive reappraisal. That is, the greater the perceived time, financial cost, or effort involved in taking protective action against phishing threats, the less that users will cope with the threat by seeing it as having a potentially positive benefit. Rather, when response costs increase, users will be less likely to focus on what they can learn from the experience and instead reduce their use of this EFC response. Therefore, in this study, we hypothesize that:

H10: Response cost negatively influences positive reappraisal.

Unlike positive reappraisal, the role of response cost in influencing threat devaluation has been investigated in a previous study on EFC in the context of security threats. Thompson et al. (2024) found that when the cost of responding to phishing threats is perceived to be higher, users are more likely to engage in threat devaluation and argued that this is because decreasing the sense of urgency allows them time before engaging in problem-focused responses. We therefore hypothesize that:

H11: Response cost positively influences threat devaluation.

Self-efficacy is an important coping appraisal factor, and increases in self-efficacy have been shown to lead to increases in intentions to protect against security threats and security behavior in many contexts (Mou et al., 2022), including protecting against phishing threats (Arachchilage and Love, 2013; Bax et al., 2021; Jansen and van Schaik, 2018; Thompson et al., 2024; Williams and Joinson, 2020); therefore, the following hypothesis is proposed:

H12: Self-efficacy positively influences phishing protection behavior.

Increased self-efficacy has been found to reduce the levels of avoidance EFC (Chen et al., 2022; Chen and Zahedi, 2016). However, Thompson et al. (2024) found that self-efficacy had a weak positive relationship with threat devaluation. Positive reappraisal shares some characteristics with threat devaluation in that it is associated with the use of problem-focused strategies in daily life (Davey, 1993), and can therefore be seen as an approach form of EFC response. Therefore, we propose that the more self-efficacy associated with protecting against phishing threats that users have, the more likely they are to engage in positive reappraisal, and the following hypothesis is proposed:

H13: Self-efficacy positively influences positive reappraisal.

As discussed above, although increases in self-efficacy have been shown to reduce the levels of avoidance EFC (Chen et al., 2022; Chen and Zahedi, 2016), Thompson et al. (2024) found that self-efficacy had a weak positive influence on threat devaluation when users are faced with phishing threats, arguing that this was the case because threat devaluation is important in situations that individuals perceive as controllable (Davey, 1993), and phishing falls into this category (Wang et al., 2016). Threat devaluation can provide mental space that allows users to prepare to cope with the threat. Therefore, in this study, we hypothesize that:

H14: Self-efficacy positively influences threat devaluation.

Liang et al. (2019) argue that it is rare for users to use positive reappraisal as a form of EFC, believing it is not relevant to the security context. However, no published previous research has considered the potential role of positive reappraisal in responding to information security threats. Given that in the health context Davey (1993) found that positive reappraisal had a positive relationship with active behavioral coping (as measured using the Health & Daily Living Form (Moos et al., 1987)), with information seeking and problem solving as significant focusses of this coping, in this study we hypothesize that positive reappraisal can lead to improved phishing protection behavior in response to phishing threats:

H15: Positive reappraisal positively influences phishing protection behavior.

Although Liang et al. (2019) found that a measure of approach EFC that included emotional support seeking and venting had a weak positive influence on user PFC behavior, in the Thompson et al. (2024) study of responses to phishing threats, threat devaluation did not have a significant effect on PFC behavior. This lack of relationship is consistent with the finding in Davey (1993) that, unlike positive reappraisal, which contributed to both active cognitive coping and active behavioral coping, threat devaluation was only associated with active cognitive coping. Given this, we hypothesize that:

H16: Threat devaluation does not influence phishing protection behavior.

4. Method

This study investigates the roles that threat devaluation and positive reappraisal play in user responses to phishing threats. The target population is adult Australians. As phishing attacks intend to steal personal information, such as banking logins, credit card details, and passwords, using an online questionnaire was appropriate to reach the population of interest. Human research ethics approval to conduct the research was obtained from Curtin University before collecting the data. The study employed the third-party survey company PollFish (www.pollfish.com) for participant recruitment. Pollfish has ESOMAR Gold Standard Data and GDPR certification. PollFish was responsible for screening panel members against the demographic requirements (age $\geq$ 18 years, residing in Australia). Eligible individuals were subsequently invited to participate. This invitation package included a comprehensive participant information sheet, a questionnaire link, and an email address for research inquiries. Data was gathered only after the participant provided consent.

Qualtrics was used to create the questionnaire, which included 53 questions. Previously validated items were used to measure the model constructs to ensure their validity and reliability; some were slightly reworded for the phishing context. For example, the Woon et al. (2005) response efficacy item 'Enabling security measures on my home wireless network will prevent hackers from stealing my identity' was reworded as 'Enabling security measures on my device will prevent hackers from stealing my identity'. Similarly, this response cost item from Woon et al. (2005), 'Enabling security features on a wireless router would be time consuming', was reworded as 'Implementing security measures on my device would be time consuming'.

All items were measured on five-point Likert scales from 'Strongly Disagree' to 'Strongly Agree'. To reduce the risk of common method bias (CMB), we used two procedural solutions: protecting participants' anonymity (Podsakoff et al., 2003) and improving items through careful construction (Podsakoff et al., 2012). Ten members of the target population pre-tested the questionnaire, and slight changes were made to the wording of several items to improve clarity and conciseness based on their feedback. To test whether CMB was an issue, the items used in the measurement model were assessed using Harman's one-factor test (Podsakoff et al., 2003). The variance explained by the first factor was 18.80 %, well below the recommended threshold of 50 %. We also did a correlational marker variable test (Lindell and Whitney, 2001). This test established that after controlling for a marker variable, all correlations that were originally significant remained significant. Therefore, CMB was unlikely to be an issue. Table A.1 provides a list of the items used to measure the constructs in the model and their sources.

We used partial least squares (PLS) to test the research model. The model was tested in two stages using SmartPLS 4 (Ringle et al., 2024). The measurement model was evaluated first, and then the structural model. Bootstrap resampling using 5000 samples was used to determine the significance of the paths in the model.

5. Results

The number of valid responses we received was 518 (54.8 % female and 45.2 % male). Table 2 provides further background information about these respondents.

We assessed the reflective measurement model by first examining the indicator loadings. Each item loaded significantly on its construct; however, there were several item loadings that were not above the recommended 0.708 (Hair et al., 2017). These items were investigated, and those with loadings below 0.65 were removed (see Table A.1). Composite reliability (CR) was used to assess internal consistency, and all constructs met the recommended level of 0.70 or above (Hair et al., 2019). Convergent validity was used to assess average variance extracted (AVE), and the AVE of each construct was above the minimum value of 0.5 (Hair et al., 2019). Table 3 lists the CR and AVE for each of the constructs in the model, showing that both internal consistency and convergent validity are satisfactory.

Discriminant validity was assessed in three ways: cross loadings, the Fornell-Larcker criterion, and the heterotrait–monotrait ratio (HTMT) of correlations criterion. All measurement items loaded more highly on their own construct than on any other construct. As shown in Table A.2, the square root of AVE for each construct was also greater than the correlation between that construct and any other construct, and all HTMT ratios are under the threshold of 0.90 (Henseler et al., 2015). Discriminant validity was therefore demonstrated with all approaches.

Coefficients of determination (R^2) and significance of path coefficients were used to evaluate the structural model. The model explained 18.6 % of the variance in fear, 39.2 % of the variance in phishing protection behavior, 40.4 % of the variance in positive appraisal, and 27.9 % of the variance in threat devaluation. Fifteen of the 16 hypotheses were supported. Fig. 2 and Table 4 summarize the results of the structural model testing.

As proposed, both perceived severity and perceived vulnerability had positive influences on fear ($\beta = 0.265$, $p < 0.001$, and $\beta = 0.261$, $p < 0.001$), and fear had a positive influence on phishing protection behavior ($\beta = 0.206$, $p < 0.001$). H1, H2, and H3 were therefore all supported. Fear was also found to influence both positive reappraisal and threat devaluation, but the effects were different. As hypothesized, when fear increased, threat devaluation decreased (H5, $\beta = -0.251$, $p < 0.001$), but positive reappraisal increased (H4, $\beta = 0.304$, $p < 0.001$). Therefore, both H4 and H5 were supported.

Hypotheses H6 to H8 relate to the role of response efficacy. As anticipated, increases in response efficacy led to increases in both phishing protection behavior ($\beta = 0.166$, $p = 0.001$) and positive reappraisal ($\beta = 0.262$, $p < 0.001$). H6 and H7 were therefore supported. Response efficacy was hypothesized to have a negative influence on

Table 2
Background information about the participants.

		Percent
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
Employment	Full time	33.8
	Part time	22.6
	Unemployed	17.2
	Student	13.5
	Retired	12.9
Experienced previous security breach?	Yes	44.8
	No	41.7
	Uncertain	13.5

Table 3
Convergent validity and AVE values.

Construct	CR	AVE
Perceived severity	0.90	0.63
Perceived vulnerability	0.81	0.52
Fear	0.83	0.62
Response efficacy	0.82	0.52
Response cost	0.79	0.56
Self-efficacy	0.79	0.56
Phishing protection behavior	0.81	0.59
Positive reappraisal	0.82	0.60
Threat devaluation	0.85	0.52

threat devaluation, and this too was confirmed ($\beta = -0.122$, $p = 0.011$), supporting H8.

Although the revised PMT (Rogers, 1983) proposes that increases in response cost are associated with increases in intention to perform protective behavior, in the information security research context (including responses to phishing threats), findings on this relationship have been mixed, and a meta-analysis by Mou et al. (2022) found no support for the role of response cost. Therefore, H9 proposed that response cost does not influence phishing protection behavior, and the non-significant relationship is consistent with this ($\beta = -0.069$, $p = 0.104$). Response cost did, however, significantly influence positive reappraisal ($\beta = -0.067$, $p = 0.040$) and threat devaluation ($\beta = 0.426$, $p < 0.001$); H10 and H11 were therefore supported.

The role of self-efficacy was explored in H12 to H14. As hypothesized, increases in self-efficacy were associated with increases in both phishing protection behavior ($\beta = 0.228$, $p < 0.001$) and positive reappraisal ($\beta = 0.230$, $p < 0.001$), providing support for H12 and H13. However, H14 was not supported, as self-efficacy did not influence threat devaluation ($\beta = 0.028$, $p = 0.544$).

Hypotheses H15 and H16 capture the proposed influence of each of the two types of EFC investigated in this research on phishing protection behavior. As hypothesized, positive reappraisal positively influenced phishing protection behavior ($\beta = 0.198$, $p < 0.001$). That is, when email users responded to phishing threats by using positive reappraisal, they were also more likely to use appropriate practical measures to counter phishing threats. Given the lack of relationship found by Thompson et al. (2024), H16 proposed that threat devaluation would not influence phishing protection behavior, and the non-significant relationship is consistent with this ($\beta = 0.001$, $p = 0.978$). Therefore, H16 was supported.

The potential role of gender in positive reappraisal and threat devaluation was also explored in this study. Mean levels of positive reappraisal were found to be significantly higher in females than males (3.85 vs 3.01, $p < 0.001$), as were mean levels of phishing protection behavior (3.75 vs 3.49, $p = 0.002$). However, there was no significant gender difference in the use of threat devaluation (2.62 vs 2.70, $p = 0.367$).

SmartPLS 4, which uses a two-stage approach to testing moderation, was used to determine whether gender had any direct or moderating influences on the use of positive reappraisal and threat devaluation (see Table 5). While gender was found to be significantly related to positive reappraisal, such that females were more likely to use positive reappraisal than males ($\beta = -0.229$, $p = 0.001$), gender did not have an impact on threat devaluation ($\beta = -0.009$, $p = 0.909$) or phishing protection behavior ($\beta = -0.066$, $p = 0.345$). Gender also did not moderate the relationships of either of the two types of EFC with phishing protection behavior.

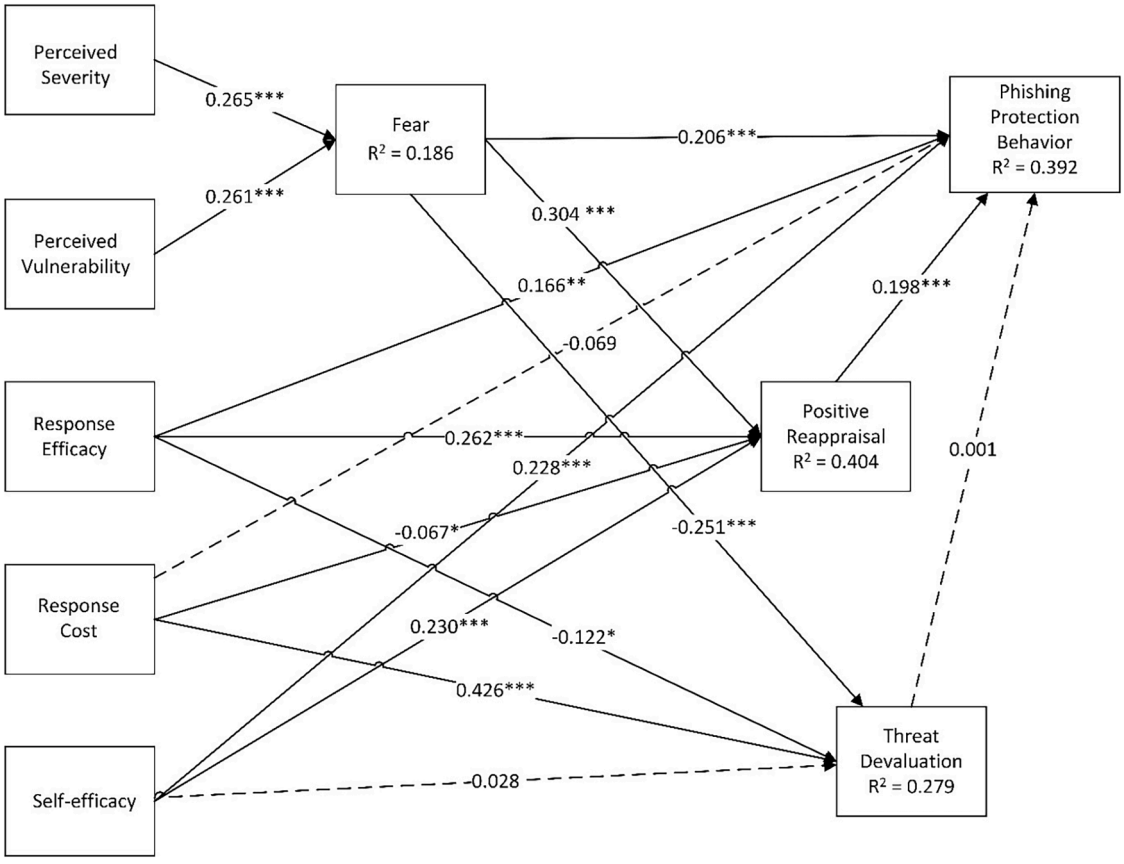

Fig. 2. Model testing results.
* $p < 0.05$. ** $p < 0.01$; *** $p < 0.001$.

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 phishing protection behavior	Supported
H4	Fear positively influences positive reappraisal	Supported
H5	Fear negatively influences threat devaluation	Supported
H6	Response efficacy positively influences phishing protection behavior	Supported
H7	Response efficacy positively influences positive reappraisal	Supported
H8	Response efficacy negatively influences threat devaluation	Supported
H9	Response cost does not influence phishing protection behavior	Supported
H10	Response cost negatively influences positive reappraisal	Supported
H11	Response cost positively influences threat devaluation	Supported
H12	Self-efficacy positively influences phishing protection behavior	Supported
H13	Self-efficacy positively influences positive reappraisal	Supported
H14	Self-efficacy positively influences threat devaluation	Not supported
H15	Positive reappraisal positively influences phishing protection behavior	Supported
H16	Threat devaluation does not influence phishing protection behavior	Supported

Table 5
Influence of gender.

	Path Coefficient	Standard Deviation	Significance
Gender → Phishing protection behavior	−0.066	0.070	0.345
Gender → Positive reappraisal	−0.229	0.067	0.001
Gender → Threat devaluation	−0.009	0.078	0.909
Gender X Positive reappraisal → Phishing protection behavior	0.014	0.078	0.853
Gender X Threat devaluation → Phishing protection behavior	−0.026	0.068	0.701

6. Discussion

When faced with a stressful situation, individuals draw from a wide repertoire of coping strategies, determined by their threat and coping appraisals. While information security literature has extensively discussed PFC responses in the form of security behavior, there is little understanding of the EFC responses that may arise from the same threat. Although Witte (1994) argued that EFC responses allow individuals to cope with fear but not with danger, and some information security work characterized all EFC under the label of *maladaptive* responses (e.g., Chen et al., 2022; Chenoweth et al., 2019; Liang and Xue, 2009), we posit that EFC responses may possess markedly different characteristics, including desirable and constructive behavior. We adopt the high-level classification of Scheier et al. (1986) to explain EFC responses in terms of their predisposition to either approach or avoid a stressful situation and specifically examine threat devaluation and positive reappraisal as coping strategies.

To situate our study within an established theoretical framework, we build upon PMT and EPPM to model how threat and coping appraisals influence security behavior and two EFC responses. We also examine how these EFC responses influence security behavior. We use phishing as the context for this study, as it is a relatively well-understood security risk, while still posing a significant and ongoing threat to end users. The results of this study provide support for 15 of the 16 hypotheses.

During primary appraisal, individual perceptions of threat severity and threat vulnerability drive phishing protection behavior through the pathway of fear, and this is covered by H1-H3. Support for these three hypotheses was found, consistent with prior studies on phishing and the broader information security domain. PMT also includes an appraisal of the coping resources available in terms of perceptions of response efficacy, response cost, and self-efficacy. We found support for our hypotheses regarding coping appraisal, thus demonstrating that our work is consistent with prior findings in these areas. Having established the consistency of our model in terms of problem-focused responses (security behavior) thus far, our major contribution is to explore the relatively uncharted domain of emotion-focused responses. Specifically, we consider the roles of threat devaluation and positive reappraisal.

We hypothesized relationships between fear (the outcome of threat appraisal) and each of the three elements of coping appraisal with EFC. Our results demonstrate that, in addition to fear having a positive influence on phishing protection behavior, it also significantly influenced the two EFC responses. Individuals with higher levels of fear demonstrated significantly higher levels of positive reappraisal (H4). These email users were more likely to try to recast the threat in terms of opportunities for personal growth and development while still taking steps to address the threat. At the same time, these individuals were significantly less likely to attempt to play down the threat by engaging in threat devaluation (H5). Thus, we find that fear can influence various types of EFC in different ways. This lends support to our theoretical position and the work of Scheier et al. (1986), suggesting that there is considerable variance among the coping responses that fall under the broad banner of EFC.

Response efficacy, a component of coping appraisal, was found to significantly influence phishing protection behavior (H6). This is consistent with prior studies on phishing (e.g., Arachchilage and Love, 2013; Bax et al., 2021; Shahbaznezhad et al., 2020; Thompson et al., 2024; Williams and Joinson, 2020) and the broader information security domain. Response efficacy also positively influenced positive reappraisal (H7). That is, when individuals felt that the courses of action available to them were effective in mitigating phishing threats, they were more likely to view the incident as a learning experience. In keeping with Folkman et al. (1986), individuals are more likely to engage in positive reappraisal for a situation that they perceive as changeable; thus, when they believe that the efficacy of their responses is high, then positive reappraisal may result. As positive reappraisal is a form of approach coping (Baker and Berenbaum, 2007), similar to phishing protection behavior, it is also associated with problem-focused responses. On the other hand, threat devaluation involves downplaying the severity of the threat as opposed to accepting its subjective reality. We found support for our hypothesis that response efficacy would negatively influence threat devaluation (H8). This is consistent with threat devaluation functioning as a form of avoidance coping. In this scenario, individuals who believed in the efficacy of the phishing responses engage less in avoidance through threat devaluation and instead engage more in adoption of both PFC and positive reappraisal.

As discussed above, response cost did not have a significant influence on phishing protection behavior (H9). Though PMT in the context of health behaviors hypothesized a link between response cost and behavior, it is apparent that this does not directly translate to the domain of information security behavior and serves as a reminder of the influence of problem context. Regarding EFC, little is known about the role of response cost. This is especially true here, given that we study forms of EFC that have not received much attention in prior information security work. We find that, as hypothesized (H10), response cost negatively influences positive reappraisal. This is explained by the nature of positive reappraisal as an approach form of coping, which is also associated with undertaking protective behavior in a health context (Davey, 1993). We suggest that as users perceive a higher cost associated with protecting themselves in terms of time, effort, or monetary value, their calculus of the benefits will, in turn, diminish. This higher response cost leads to a lower positive reappraisal. At the same time, these perceptions of higher cost positively influence levels of threat devaluation (H11). By engaging in threat devaluation in situations with high response cost, users may decrease the sense of urgency and free up

resources to deal with the problem in other ways (Thompson et al., 2024).

Self-efficacy, the individual's belief that they can undertake protective behaviors, is an established element of coping appraisal and a core element of Social Cognitive Theory (Bandura, 1997). Consistent with prior behavioral information security work (Mou et al., 2022), including studies on phishing (Arachchilage et al., 2016), we found that self-efficacy had a positive influence on phishing protective behavior (H12). In the context of EFC, we found that self-efficacy also positively influences levels of positive reappraisal (H13). Prior work from the health domain has shown that positive reappraisal is associated with problem-focused strategies (Davey, 1993). As positive reappraisal is an approach form of EFC, it involves engaging with the problem and can lead to desirable outcomes. Similarly, Freire et al. (2020) found that general self-efficacy was strongly correlated with positive reappraisal and suggested that this is a valuable mechanism for both reducing stress and motivating behavioral responses.

On the other hand, we did not find the same influence of self-efficacy on threat devaluation, in contrast with our hypothesis (H14) and the findings of Thompson et al. (2024). As threat devaluation is important in controllable situations (Davey, 1993), and we believe phishing falls into this category, we had expected threat devaluation to also increase with self-efficacy. An explanation for this is found in our characterization of approach vs avoidance EFC. If threat devaluation is being adopted as an avoidance EFC, in that the individual is downplaying the reality of the threat, then our findings are consistent with earlier studies in information security behavior (Chen et al., 2022; Chen and Zahedi, 2016). We believe that certain types of EFC, such as threat devaluation, may be highly context dependent as they possess elements of both approach and avoidance coping. Thus, the specific details of the threat may determine whether approach or avoidance characteristics are expressed. As more is learned about the impact of specific coping strategies in the face of security threats, there is potential to explore how these strategies interact and how they are selected and applied. Studies in the healthcare context have considered the role of this flexibility in coping (Haythornthwaite et al., 1998), suggesting that flexibility enhances perceptions of control over the stressors, which may in turn influence self-efficacy beliefs, thus paving the way for a feedback loop between response and perceptions. This is therefore a promising area for future research.

Understanding the way in which coping strategies are selected and applied may also provide insights into the concept of resilience, a topic that is of interest to the information security community (McCormac et al., 2018). According to Cheng and Cheung (2005), individuals with less flexible coping styles have fewer strategies available, making them less effective at adapting to the specific challenges of a situation. This finding aligns with Hobfoll's conservation of resources theory (Hobfoll et al., 2018). The theory posits that individuals rich in personal resources—such as varied approach coping strategies—engage in an upward spiral where they continually acquire, develop, and protect new resources. Conversely, facing a challenge with scarce resources (e.g., low coping flexibility) initiates a downward spiral of resource loss, making the individual more vulnerable to stress.

We considered the influence of both types of EFC on phishing protection behavior to understand if, and to what extent, there is a beneficial aspect to EFC. Consistent with our hypothesis, positive reappraisal has a significant positive influence on phishing protection behavior (H15). This is a noteworthy finding as we challenge the notion that EFC is maladaptive and suggest that it may be a relevant and productive element of a successful coping strategy. Threat devaluation (H16), on the other hand, has a different function, and we did not hypothesize that it would have the same impact on protective behavior. Our hypothesis in this instance was also confirmed. Threat devaluation contributes to active cognitive coping with a phishing threat, but not active behavioral coping.

Finally, we conducted post-hoc exploratory analysis on any potential gender differences in the EFC styles. Gender has a significant influence on positive reappraisal, where female respondents were more likely to engage in positive reappraisal. There was no such influence found on threat devaluation, nor was gender found to moderate the relationships between EFC and phishing protection behavior. This finding mirrors observations in the health domain where women were found to be more likely to engage in positive reappraisal, and also more likely to benefit from this strategy (Nowlan et al., 2015). Indeed, of the gender differences noted in early work on EFC, positive reappraisal has emerged as a consistent factor (Folkman et al., 1987). It has been suggested that gender differences in the adoption of EFC strategies may be socially constructed through the roles that males and females may occupy (Garza Varela et al., 2021). Matud (2004) suggests that gender differences may also be explained by the kind of situations or stressors that males or females encounter. However, in the context of our study, the stressor (phishing threat) is constant across the entire cohort; thus this explanation does not suffice. A more likely explanation arises from the socialization hypothesis, whereby females may have been socialized to adopt more emotion-focused behaviors (Pearlin and Schooler, 1978). Here, it is important to note that the adoption of positive reappraisal is found to be a beneficial and desirable strategy as it remains highly linked to phishing protection behavior.

6.1. Implications for theory and practice

The emphasis on information security behavior as the variable of interest, though vital, leaves a gap in the theoretical understanding of the role of EFC in information security research. As PMT, the most popular theoretical foundation for behavioral information security (Haag et al., 2021; Hassandoust et al., 2020), does not explicitly accommodate EFC, this gap is further reinforced as newcomers and experienced researchers alike tend to base their work on the established and accepted theoretical foundations. EPPM and Parallel Response Model (Leventhal, 1970, 1971) both provide a mechanism to accommodate a wider range of information security responses by explicitly considering the role of emotion-focused responses. These models describe how, in response to a threat, an individual may undertake either problem-focused (termed danger control) or emotion-focused (termed fear control) processes. However, there has been relatively little uptake in the information security realm. Our first theoretical contribution is the development of a research model that builds on PMT and includes components of EFC to demonstrate the influence of threat and coping appraisal processes on internal self-regulation.

Secondly, we consider a new type of EFC that has not been examined in this context before – positive reappraisal. This is a significant contribution, as prior work has typically focused on EFC such as avoidance or denial, which are generally in conflict with the security behavior of interest. Though this prior work provides an interesting contrast, it fosters the perception that EFC is by nature maladaptive and to be prevented. For example, the highly influential TTAT (Liang and Xue, 2009) considered maladaptive EFC and consequently describes EFC as "oriented toward creating a false perception of the environment without actually changing it" (p.78). We provide an alternate perspective by considering the role of an approach related EFC, and we show this to be linked to protective behavior. Our findings regarding positive reappraisal are that it has a positive influence on PFC, and most significantly, it does *not* involve changing the objective reality of the threat. Furthermore, it is hoped that this theoretical contribution will reveal a new avenue for improving security behavior via the pathways of EFC.

Our adoption of the approach versus avoidance dimensions of EFC provides a theoretical structure for the proposition that PFC and EFC cannot be considered as homogeneous entities. Specifically, we find evidence that various EFC strategies are influenced differentially by threat and coping appraisals and, in some cases, may have a link to PFC. Notably, in our examination of threat devaluation, we discovered that the approach versus avoidance classification is not always clear-cut, as threat devaluation possesses some but not all elements of avoidance.

Though prior work on this is scarce, we note that the findings are mixed and take this as possible evidence of the context-dependent nature of coping responses. We have thus far only considered the appraisal processes leading to coping; however, coping is a process that develops in the context of a particular situation (Lazarus and Folkman, 1984). Evidence from the psychological sciences suggests that coping is sensitive to environmental resources and conditions in the same way that it is sensitive to internal appraisal processes (Folkman and Moskowitz, 2004), yet this has not been observed or tested in information security work. Thus, our third theoretical contribution is the introduction of the concept of context dependency of specific coping strategies, and it is one that is a viable avenue for continued investigation.

A practical implication arises from our investigation of approach related EFC (positive reappraisal), and the finding that it may motivate protective behavior. This finding creates new opportunities for practical behavioral change through targeting and encouraging specific EFC mechanisms, which are known to be beneficial, rather than assuming that non-PFC behavior is all bad. Security education and training awareness programs should include material on EFC to help users understand which types of EFC responses are likely to be helpful and which may reduce their ability to protect themselves against security threats.

While positive reappraisal does not include changing the objective reality of the threat, it does involve changing the way in which the event is construed, or the goals of the individual (Uusberg et al., 2019). In information security practice, the goal of preventing cyberattacks might be considered self-evident and quite high-level in nature. However, goals vary in both salience and motivational impact (Huang and Bargh, 2014), so a broad goal such as “stay safe online” may provide little opportunity for the individual to assess or acknowledge their success. More specific and context-based framing, such as "spot a potential phishing message," may provide the needed opportunity for the individual to acknowledge the productive and learning opportunities and to recast through positive reappraisal. This is a strategy which, to our knowledge, has not been applied before in an information security context.

Several limitations of this study should be addressed in future work. As the research was limited to user responses to phishing threats, the applicability of the model in other security contexts should be confirmed in the future. Similarly, the research could be extended to consider the roles of other EFC responses such as wishful thinking, denial, and emotional support seeking. Although the analysis did not suggest common method issues, because all constructs in the proposed model were measured through self-report, CMB is possible. Future research on EFC responses to security threats should include further procedural steps to reduce the potential for this issue, such as the use of more objective behavioral measures of protection behavior. The use of self-report measures, though standard in studies of this nature, does carry some risk of biased responses. While we have made attempts to mitigate social desirability bias through having an anonymous survey, other biases might be alleviated through objective behavioral measures. As these were not logistically feasible at the scale required for this study, it remains an interesting avenue for future work and development.

7. Conclusion

Users may respond to information security threats with a range of coping strategies in addition to information security behavior that directly protects them. However, relatively little is known about the roles of emotion-focused responses, and prior work has often considered these to be maladaptive. We study the roles of two EFC responses in how users respond to information security threats. Our research proposes and tests a model of how positive reappraisal and threat devaluation are influenced by factors that play a role in phishing protection behavior, and in turn how positive reappraisal and threat devaluation influence phishing protection behavior.

We find that many determinants of phishing protection behavior also influence whether users undertake positive reappraisal of the threat or devalue it. Positive reappraisal had a positive influence on phishing protection behavior, but this was not the case with threat devaluation. Based on the findings, we conclude that the effects of EFC responses are nuanced and classify them according to whether the individual response is to either approach or avoid the threat. We also pave the way for future work to explore the relationship between these EFC responses and other outcomes beyond the phishing protection context of this study. This study also explored whether gender plays a role in the use of the two types of EFC response considered in the study, and we found that women were more likely to use positive reappraisal than men, but no gender differences in the use of threat devaluation were found.

Our findings contribute to the understanding of a little-researched area of information security and create new opportunities for practical behavioral change through targeting and encouraging specific EFC mechanisms which are known to be beneficial, rather than assuming that non-PFC behavior is always problematic.

CRediT authorship contribution statement

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

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.

Appendix

Tables A1 and A2.

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	

(*continued on next page*)

Table A.1 (*continued*)

Item	SouSource
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)
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)
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)
Response cost	
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)
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)
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)
Phishing protection 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 analyze for phishing indicators	Wang et al. (2017)
I try to concentrate on the task while opening emails	Wang et al. (2017)
Positive reappraisal	
I would learn to protect my data better in the future	Carver et al. (1989)
It would be a learning experience for me	Carver et al. (1989)
I might get inspired to find ways to protect others	Folkman et al. (1986)
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
Discriminant validity.

	PS	PV	F	RE	RC	SE	PPB	PR	TD
Perceived severity (PS)	**0.795**								
Perceived vulnerability (PV)	0.343	**0.718**							
	(0.434)								
Fear (F)	0.354	0.352	**0.788**						
	(0.452)	(0.498)							
Response efficacy (RE)	0.502	0.343	0.399	**0.724**					
	(0.649)	(0.478)	(0.576)						
Response cost (RC)	−0.114	0.080	−0.003	−0.043	**0.751**				
	(0.159)	(0.140)	(0.129)	(0.083)					
Self-efficacy (SE)	0.484	0.249	0.328	0.577	−0.108	**0.751**			
	(0.663)	(0.367)	(0.494)	(0.879)	(0.177)				
Phishing protection behavior PPB)	0.493	0.252	0.443	0.485	−0.122	0.495	**0.770**		
	(0.656)	(0.365)	(0.649)	(0.712)	(0.189)	(0.779)			
Positive reappraisal (PR)	0.510	0.344	0.485	0.520	−0.104	0.489	0.502	**0.771**	
	(0.672)	(0.500)	(0.710)	(0.760)	(0.161)	(0.755)	(0.762)		
Threat devaluation (TD)	−0.341	−0.162	−0.292	−0.224	0.429	−0.170	−0.221	−0.283	**0.72**3
	(0.415)	(0.206)	(0.386)	(0.299)	(0.616)	(0.244)	(0.300)	(0.386)	

Numbers in bold on diagonal are the square roots of AVE.
Numbers inside brackets are HTMT.
Other numbers are correlations.

Data availability

The authors do not have permission to share data.

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. https://doi.org/10.1109/ISI.2016.7745462.

Alrawhani, E.M., Binti, R.A., A, A.-S.M., & and Alkawsi, G. (2025). Integrating information security culture and protection motivation to enhance compliance with information security policies in banking: evidence from PLS-SEM and fsQCA. *Int. J. Hum.–Comput. Interact.*, 1–22. 10.1080/10447318.2025.2464900.

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, 2024. Phishing Act. Trends Rep.: 4th Quart. 2024. https://apwg.org/trendsreports/.

Arachchilage, N.A.G., Love, S., 2013. A game design framework for avoiding phishing attacks. Comput Hum. Behav 29, 706–714. https://doi.org/10.1016/j.chb.2012.12.018.

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

Baker, J.P., Berenbaum, H., 2007. Emotional approach and problem-focused coping: a comparison of potentially adaptive strategies. Cogn. emot. 21 (1), 95–118. https://doi.org/10.1080/02699930600562276.

Bandura, A., 1997. Self-efficacy: The exercise of Control. Macmillan.

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.

Bechara, A., Damasio, A.R., Damasio, H., Anderson, S.W., 1994. Insensitivity to future consequences following damage to human prefrontal cortex. Cognition 50 (1), 7–15. https://doi.org/10.1016/0010-0277(94)90018-3.

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. Manag. 66 (4), 552–567. https://doi.org/10.1109/TEM.2018.2835461.

Chen, Y., Luo, X., Li, H., 2022. Beyond adaptive security coping behaviors: theory and empirical evidence. Inf. Manag. 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.

Cheng, C., Cheung, M.W., 2005. Cognitive processes underlying coping flexibility: differentiation and integration. J. Pers. 73 (4), 859–886.

Chenoweth, T., Gattiker, T., Corral, K., 2019. Adaptive and maladaptive coping with an IT threat. Inf. Syst. Manag. 36, 24–39. https://doi.org/10.1080/10580530.2018.1553647.

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. IEEE.

Cho, H., Li, P., Goh, Z., 2020. Privacy risks, emotions, and social media. ACM Trans. Comput.-Hum. Interact. 27, 1–28. https://doi.org/10.1145/3412367.

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.

Flores-Torres, J., Gómez-Pérez, L., McRae, K., 2022. Positive cognitive reappraisal is beneficial for women's but not for men's IGT decision-making. Motiv. Emot. 46 (3), 350–365. https://doi.org/10.1007/s11031-022-09927-4.

Folkman, S., 1988. Ways of Coping Questionnaire, Sampler set, Manual, Test Booklet, Scoring Key. Consulting Psychologists Press.

Folkman, S., Lazarus, R.S., 1980. An analysis of coping in a middle-aged community sample. J. Health Soc. Behav. 21 (3), 219–239. https://doi.org/10.2307/2136617.

Folkman, S., Lazarus, R.S., 1985. If it changes it must be a process: a study of emotion and coping during three stages of a college examination. J. Pers. Soc. Psychol. 48 (1), 150–170. https://doi.org/10.1037/0022-3514.48.1.150.

Folkman, S., Lazarus, R.S., Dunkel-Schetter, C., DeLongis, A., Gruen, R.J., 1986. Dynamics of a stressful encounter: cognitive appraisal, coping, and encounter outcomes. J. Pers. Soc. Psychol. 50 (5), 992–1003. https://doi.org/10.1037/0022-3514.50.5.992.

Folkman, S., Lazarus, R.S., Pimley, S., Novacek, J., 1987. Age differences in stress and coping processes. Psychol. Aging 2 (2), 171.

Folkman, S., Moskowitz, J.T., 2000. Positive affect and the other side of coping. Am. psychol. 55 (6), 647–654. https://doi.org/10.1037/0003-066X.55.6.647.

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

Freire, C., Ferradás, M.d.M., Regueiro, B., Rodríguez, S., Valle, A., Núñez, J.C., 2020. Coping strategies and self-efficacy in university students: a person-centered approach. Front. Psychol. 11. https://doi.org/10.3389/fpsyg.2020.00841. Article 841.

Freud, S., 1915. Instincts and their vicissitudes. In: The Standard Edition of the Complete Psychological Works of Sigmund Freud, 14, pp. 117–140.

Garza Varela, J.P., Leija Guerrero, J.G., Sánchez Rodríguez, K.E., Kawas Valle, O., Cruz-de la Cruz, C.d.l., 2021. Positive reappraisal as a stress coping strategy during the COVID-19 pandemic. Salud ment. 44 (4), 177–184.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. Comput. Secur. 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015.

Haag, S., Siponen, M., Liu, F., 2021. Protection motivation theory in information systems security research: a review of the past and a road map for the future. ACM SIGMIS Database: DATABASE Adv. Inf. Syst. 52 (2), 25–67. https://doi.org/10.1145/3462766.3462770.

Hair, J., Risher, J., Sarstedt, M., Ringle, C., 2019. When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. 31 (1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203.

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

Hakim-Larson, J., Murdaca, L., Dunham, K., Vellet, S., Levenback, J., 1999. Parental affect and coping. Can. J. Behav. Sci. 31 (1), 5–18. https://doi.org/10.1037/h0087069.

Hassandoust, F., Techatassanasoontorn, A.A., Singh, H., 2020. Information security behaviour: a critical review and research directions. ECIS 2020 Research Papers. https://aisel.aisnet.org/ecis2020_rp/71.

Haythornthwaite, J.A., Menefee, L.A., Heinberg, L.J., Clark, M.R., 1998. Pain coping strategies predict perceived control over pain. Pain. 77 (1), 33–39. https://doi.org/10.1016/S0304-3959(98)00078-5.

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

Hobfoll, S.E., Halbesleben, J., Neveu, J.-P., Westman, M., 2018. Conservation of resources in the organizational context: The reality of resources and their consequences. Annu. Rev. Organ. Psychol. Organ. Behav. 5, 103–128.

Huang, J.Y., Bargh, J.A., 2014. The selfish goal: autonomously operating motivational structures as the proximate cause of human judgment and behavior. Behav. Brain Sci. 37 (2), 121–135.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F., 2007. Social phishing. Commun ACM 50 (10), 94–100.

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.

Lazarus, R.S., 1966. Psychological Stress and the Coping Process. McGraw-Hill.

Lazarus, R.S., Folkman, S., 1984. Stress, appraisal, and Coping. Springer.

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. https://doi.org/10.2105/AJPH.61.6.

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., 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. https://www.jstor.org/stable/26847869.

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.

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. https://aisel.aisnet.org/thci/vol3/iss3/2.

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. In: Proceedings of HICSS 2021, pp. 6691–6700. https://doi.org/10.24251/HICSS.2021.803.

Matud, M.P., 2004. Gender differences in stress and coping styles. Pers. Individ. Dif. 37 (7), 1401–1415.

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., Lillie, M., 2018. The effect of resilience and job stress on information security awareness. Inf. Comput. Secur. 26 (3), 277–289. https://doi.org/10.1108/ics-03-2018-0032.

McGill, T., Thompson, N., 2021. Exploring potential gender differences in information security and privacy. Inf. Comput. Secur. 29 (5), 850–865. https://doi.org/10.1108/ICS-07-2020-0125.

Moos, R.H., Cronkite, R.L., Billings, A.G., Finney, J.W., 1987. Revised Health and Daily Living form Manual. Veterans Administration and Stanford University Medical Centers.

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. https://doi.org/10.17705/1CAIS.04207.

Nowlan, J.S., Wuthrich, V.M., Rapee, R.M., 2015. Positive reappraisal in older adults: a systematic literature review. Aging Ment. Health 19 (6), 475–484. https://doi.org/10.1080/13607863.2014.954528.

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. https://doi.org/10.1037/0021-9010.88.5.879.
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., Becker, J.-M., 2024. SmartPLS 4. In SmartPLS. https://www.smartpls.com.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91 (1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.
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, pp. 153–176.
Scheier, M.F., Weintraub, J.K., Carver, C.S., 1986. Coping with stress: divergent strategies of optimists and pessimists. J. Pers. Soc. Psychol. 51 (6), 1257–1264. https://doi.org/10.1037/0022-3514.51.6.1257.
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.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J., 2010. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp. 372–382.
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.
Sutton, A., Tompson, L., 2025. Towards a cybersecurity culture-behaviour framework: a rapid evidence review. Comput. Secur. 148, 104110. https://doi.org/10.1016/j.cose.2024.104110.
Thompson, N., McGill, T., Narula, N., 2024. No point worrying" – The role of threat devaluation in information security behavior. Comput. Secur. 143, 103897. https://doi.org/10.1016/j.cose.2024.103897.
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.
Tobin, D.L., Holroyd, K.A., Reynolds, R.V., Wigal, J.K., 1989. The hierarchical factor structure of the Coping Strategies Inventory. Cogn. Ther Res 13, 343–361. https://doi.org/10.1007/BF01173478.
Uusberg, A., Taxer, J.L., Yih, J., Uusberg, H., Gross, J.J., 2019. Reappraising reappraisal. Emot. Rev. 11 (4), 267–282. https://doi.org/10.1177/1754073919862617.
van 't Riet, J., Ruiter, R.A.C., 2013. Defensive reactions to health-promoting information: an overview and implications for future research. Health Psychol. Rev. 7 (sup1), S104–S136. https://doi.org/10.1080/17437199.2011.606782.
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 Hum. Behav 101, 286–296. https://doi.org/10.1016/j.chb.2019.07.034.
Wang, J., Li, Y., Rao, H.R., 2016. Overconfidence in phishing email detection. J. Assoc. Inf. Syst. 17 (11). https://doi.org/10.17705/1jais.00442.
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. https://doi.org/10.1287/isre.2016.0680.
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 Hum. Behav 24, 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005.
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. https://doi.org/10.1080/0144929X.2021.1954242.