Behaviour & Information Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats

Tong Xin, Mikko Siponen & Sihua Chen

To cite this article: Tong Xin, Mikko Siponen & Sihua Chen (2021): Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats, Behaviour & Information Technology, DOI: 10.1080/0144929X.2021.1954242

To link to this article: https://doi.org/10.1080/0144929X.2021.1954242

Published online: 25 Jul 2021.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2021.1954242

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats

Tong Xin[a], Mikko Siponen[a] and Sihua Chen[b]

[a]Faculty of Information Technology, University of Jyväskylä, Jyvaskyla, Finland; [b]Faculty of Information Management, Jiangxi University of Finance and Economics, Nanchang, People's Republic of China

ABSTRACT

According to coping theory, individuals cope with information system threats by adopting either problem-focused coping (PFC) or emotion-focused coping (EFC). However, little is known about EFC in the information security (ISec) literature. Moreover, there is potential confusion regarding the meaning of some EFC strategies. Hence, ISec scholars and practitioners may (i) have a narrow view of EFC or (ii) confuse it with other concepts. In this study, we offer one response to this issue. We first address the ambiguity regarding EFC before differentiating five inward EFC strategies and assessing them empirically in the mobile malware context. To the best of our knowledge, this study is the first to compare several inward EFC strategies in the ISec field.We contribute two new findings on EFC: 1) response efficacy is a crucial factor that impedes users from implementing EFC strategies; 2) avoidance and fatalism significantly impede PFC. Our study also contributes to the ISec literature by categorising EFC into active and passive forms. We showed that individuals' use of passive inward EFC strategies was positively associated with threat vulnerability. Finally, we provide interesting insights into the complicated responses of individuals to mobile malware threats, presenting implications for ISec research and practice.

ARTICLE HISTORY
Received 8 November 2020
Accepted 6 July 2021

KEYWORDS
Inward emotion-focused coping; coping theory; protection motivation theory; information security behaviour

1. Introduction

The ubiquity of the Internet, computers, and mobile devices exposes personal computer users to numerous information security (ISec) threats. Unfortunately, users' risky information security behaviour[1] is a factor in ISec incidents (Johnston, Warkentin, and Siponen 2015; Moody, Siponen, and Pahnila 2018). For example, according to recent reports, 23% of data breaches (IBM 2019) and 50% of data leak incidents (2020 Cyber Threats 2020) were caused by human behaviour. In 2020, the average total cost of data breaches due to human error was 3.33 million USD (IBM 2019). Thus, a key research stream pertains to understanding information behaviours or intentions (Moody, Siponen, and Pahnila 2018).

According to coping theory, two broad streams of coping mechanisms are related to ISec threats: problem-focused coping (PFC) and emotion-focused coping (EFC) (Lazarus and Folkman 1984). In general, users' risk-taking responses to information security (ISec) threats are considered related to EFC (Liang et al. 2019). The other form of coping is PFC, which refers to an individual's response that deals directly with actual threats (Lazarus and Folkman 1984; Liang and Xue 2009; Liang et al. 2019). Hence, the response of installing anti-malware software can be considered PFC. In contrast, ignoring any anti-malware software would constitute EFC, or a risky behaviour intended to reduce emotional distress rather than directly manage actual threats (Rogers, Prentice-Dunn, and Gochman 1997). Because a key concern in ISec behavioural research is risky behaviour, regardless of whether it is labelled ISec awareness (Siponen 2000), information security policy violations (Vance, Siponen, and Pahnila 2012), or computer abuse/misuse (Jung et al. 2016), EFC is highly important (Liang and Xue 2009, 2010).

EFC[2] can be divided into inward and outward (Liang et al. 2019). Inward EFC is an impediment to ISec protection behaviour because it promotes risky information behaviour (Chenoweth, Minch, and Gattiker 2009; Liang and Xue 2010; Chen and Zahedi 2016; Liang et al. 2019). Inward EFC suppresses the generation of negative emotions by ignoring or distorting the perception of ISec threats, but it does not reduce the negative effects of emotions and stress in order to promote rational behaviour (Liang et al. 2019).

Despite the role of inward EFC in risky or insecure actions (Liang et al. 2019), only the inward EFC strategies of avoidance, reactance, psychological distancing,

CONTACT Tong Xin toxin@student.jyu.fi Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, Jyvaskyla, FI-40014, Finland

and wishful thinking have been investigated in previous ISec studies (Chenoweth, Minch, and Gattiker 2009; D'Arcy, Herath, and Shoss 2014; Lowry and Moody 2015; Chen and Zahedi 2016; Moody, Siponen, and Pahnila 2018; Liang et al. 2019). To the best of our knowledge, other inward EFC strategies remain unstudied and therefore unrecognised in the ISec literature. This is noteworthy because the role of EFC is highly important in understanding and further addressing risky ISec behaviours. For example, users who know that there is a risk of data transmission but still use non-secured WI-FI may adopt different inward EFC strategies. One set of users may believe that the risk does not apply to them (i.e. wishful thinking), while others may guess that the risk is governed by bad luck, and they can do nothing to avoid it (i.e. fatalism). The cognitive factors that trigger users to adopt different inward EFC strategies may also be diverse. The lack of critical knowledge also has implications for practitioners in conducting ISec education. For example, if practitioners' understanding of inward EFC remains narrow, they may ignore some factors (e.g. perceived threat vulnerability) that have not been shown in previous ISec studies to significantly affect avoidance and reactance but are likely to affect previously uninvestigated strategies.

To address the issues related to inward EFC strategies and answer the research question, '*How do different inward EFC strategies affect individual users' ISec behaviours?*' we conducted a study to examine five inward EFC strategies. Informed by coping theory and protection motivation theory (PMT), we conceptualised and operationalised five inward EFC strategies and distinguished them at the theoretical level. In addition, we sought to clarify confusing points that could have obscured researchers' and practitioners' understanding of EFC and related concepts. For instance, Liang and Xue (2010) examined avoidance, defining it as a PFC (79). However, previous ISec studies (e.g. Moody, Siponen, and Pahnila 2018) have conflated Liang and Xue's (2010) definition of 'avoidance' with the EFC strategy. Analysing data collected from 406 individual users in China, we empirically compared the effects of these inward EFC strategies on their PFC behaviour, including the role of cognitive factors. This study contributes to the scant body of knowledge of EFC in the extant ISec behavioural literature, which could help researchers understand and address individuals' risky ISec behaviour and recommends future directions for ISec research on inward EFC. We believe that the results of this study will also be valuable for ISec practitioners.

The rest of the paper is organised as follows. In the literature review, we elaborate on the basic factors of coping and EFC before discussing the existing literature on information behaviour. In the third section, we present the research hypotheses and models. In Section 4, we describe the research method used to collect and analyse the data and test our hypotheses. In the concluding section, we discuss the results of our analysis, the limitations of the study, and its contributions to the literature. Finally, we recommend directions for future research.

2. Literature review: coping and ISec studies on EFC

This literature review includes two sub-sections. In Section 2.1, we explain coping and EFC in general. In Section 2.2, we review and attempt to clarify the confusion regarding EFC strategies in the existing ISec literature on EFC.

2.1. Coping

Coping has been defined as 'cognitive and behavioural efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person' (Lazarus and Folkman 1984, 141). Coping plays a significant role in the process of psychosocial adaptation to stressors. Rather than a unidimensional behaviour, coping is an organisational construct that functions at several levels and contains 'a plethora of behaviours, cognitions, emotions and perceptions' (Pearlin and Schooler 1978, 7–8) that individuals use to deal with external stressors and psychological stress. As illustrated in Figure 1, the structure of coping can be considered hierarchical (Carver, Scheier, and Weintraub 1989; Lazarus 1993).

As shown in Table 1, three broad levels of coping can be conceptualised. The highest level of coping involves 'strategies of adaptation' that serve larger evolutionary functions (Witte 1994), such as escaping from potentially dangerous situations. At this level, coping includes adaptive processes that are interposed between stress and its physiological, psychological, and social effects. The lowest level of coping comprises a myriad of situation-determined coping 'instances' or real-time responses that individuals use in dealing with specific stresses, such as taking medicine during a cold or wearing amulets before surgery.

The intermediate level of coping refers to a coherent set of categories of highly personal responses and their functions in regulating the effects of stress. Skinner et al. (2003) suggested that two types of individual coping classifications belong to the intermediate level. One coping type involves a set of lower-order categories labelled 'coping strategies,' in which different instances of coping are classified into clear, mutually exclusive

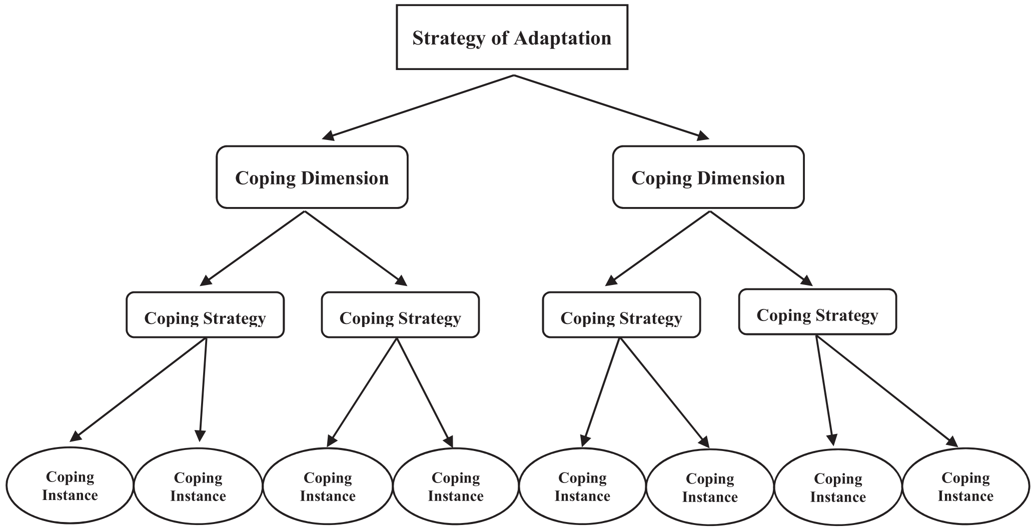

Figure 1. Conceptualisation of the structure of coping. Adapted from Skinner et al. (2003).

categories (e.g. problem solving, avoidance, and fatalism). These lower-order categories can be classified and embedded in a set of higher-order categories labelled 'dimensions of coping.' For example, classifications in the intermediate level of coping, namely, lower-order coping strategies, such as fatalism and avoidance, can be assigned to the EFC classification, which is a coping dimension (McCrae and Costa 1986). This coping classification is more multifunctional and multidimensional compared with the lower-order one (Skinner et al. 2003).

At present, the most widely used classifications of coping dimensions in ISec research may be PFC and EFC, which are distinguished according to their coping functions (Lazarus 1966; Folkman and Lazarus 1980). PFC is directed at 'managing or altering the problem causing the distress,' whereas EFC aims at 'regulating the emotional response to the problem' (Lazarus and Folkman 1984, 150). As Liang and Xue (2009) noted, these two coping styles are not mutually exclusive; they can be elicited by stressors simultaneously. PFC tends to predominate when individuals believe that something can be done to manage the stressor (Lazarus and Folkman 1984). In contrast, EFC tends to predominate when individuals feel that there is no other way to deal with the stressor than to endure it (Lazarus and Folkman 1984).

However, PFC and EFC are not antagonistic; both are adaptive ego-defence mechanisms (Rippetoe and Rogers 1987). According to Lazarus (1993), adaptive refers to 'the effectiveness of coping in improving the adaptational outcome' (237). If the coping outcome achieves the goal of adapting to external stressors or mediating internal conflicts, then the coping is adaptive. For example, individuals may reduce the negative emotions caused by a malware threat by ignoring it. In this case, ignoring the malware threat is adaptive because it manages stress. However, it can be considered a maladaptive response if the goal is ISec protection.

2.2. Information behaviour research and EFC

This research is based on three areas that could benefit further research and clarification in research on EFC in ISec. First, although EFC is an essential component in existing theoretical frameworks (e.g. PMT, EPPM) that are widely cited in ISec behavioural research, there is little discussion of it in the literature. Our review of the relevant literature revealed that six information behaviour studies have examined EFC empirically (Table 2). It was recommended that two coping mechanisms, PFC and EFC, should be combined to understand users' ISec behaviour (Witte 1992; Rogers, Prentice-Dunn, and Gochman 1997). In particular, inward EFC may be one reason for individuals' risky ISec behaviour. It has been shown to significantly impede PFC (Chenoweth, Minch, and Gattiker 2009; Liang et al. 2019). Because of the gap in previous research on this topic, it is necessary to conduct an in-depth study on EFC, especially inward EFC strategies.

Next, the concepts underpinning some EFC strategies were unclear or ambiguous in the ISec literature. For example, Moody, Siponen, and Pahnila (2018) defined avoidance as a 'maladaptive coping mechanism characterised by the effort to avoid dealing with a stressor' according to the extended parallel process model and technology threat avoidance theory (TTAT) (289). However, Moody, Siponen, and Pahnila (2018) definition of avoidance was inconsistent with that of

Table 1. Structure of Coping.

Level		Name	Conceptualisation	Example
High level		Strategy of adaptation	Basic adaptive processes interposed between stress and its outcomes from physiological, psychological, and social aspects.	Escaping from potentially dangerous situations
Intermediate level	Higher	Coping dimensions	A set of higher-order categories of highly personal responses that regulate the effects of stress. Coping strategies are classified and nested into this level.	Problem-focused coping, approach, engagement
	Lower	Coping strategies	A set of lower-order categories of personal responses that regulate the effects of stress. Different instances of coping are classified into clear, mutually exclusive categories at this level.	Problem solving, avoidance, fatalism
Low level		Coping instances	A multitude of situation-determined coping 'instances' or real-time responses that individuals use when dealing with specific stresses	Taking medicine after a cold, wearing amulets before surgery

TTAT, which should have been explained to avoid further ambiguity regarding the definition. In TTAT, avoidance is considered PFC, which refers to adaptive behaviour that avoids dealing with malicious information technology (IT) threats (Liang and Xue 2009, 2010). Moody, Siponen, and Pahnila (2018) confused the TTAT definition of avoidance as adaptive and maladaptive avoidance, which, however, is understandable because avoidance could be EFC in most cases.

Some ISec authors used the term avoidance to represent all EFC strategies. For example, Chenoweth, Minch, and Gattiker (2009) used EFC as a variable in their model. However, they actually measured avoidance. To clarify, this point is not meant as a critique of Chenoweth, Minch, and Gattiker (2009), but readers may have inferred from Chenoweth, Minch, and Gattiker (2009) that EFC is the same as avoidance, when in fact, avoidance is only one type of EFC. Moreover, Chen and Zahedi (2016) defined avoidance as 'avoiding using the Internet in varying degrees, especially avoiding sensitive activities' (206). In their study, the definition of avoidance was 'different from emotional-focused coping (e.g. denial or helplessness) discussed in TTAT' (Liang and Xue 2009, 210). However, avoidance, as defined by Chen and Zahedi (2016), can be understood as both PFC and EFC. On one hand, avoidance is PFC because avoiding the use of the Internet can effectively disregard online security threats in the short term. On the other hand, in the long term, it is EFC when individuals need to use the Internet but do not because they fear threats.

D'Arcy, Herath, and Shoss (2014) examined three emotion-focused responses: (i) reconstrue conduct, (ii)

Table 2. Empirical Information Behaviour Studies on EFC.

Study	Context	EFC constructs	Theory	Method	Key findings related to EFC
Liang et al. (2019)	Study how individuals cope with IT security threats by taking into account both PFC and EFC.	Distancing; Denial; Wishful thinking; Venting; Emotional support seeking	Coping theory	Survey; experiment	EFC is divided into two categories: inward and outward, inward EFC impedes PFC, outward EFC facilitates PFC
Moody, Siponen, and Pahnila (2018)	Combined 12 well-known theories in the ISec field to build a unified model of ISEC POLICY compliance.	Avoidance; Reactance	PMT, EPPM	Survey	Reactance was positively influenced by fear and neutralisation.
Chen and Zahedi (2016)	Compared individuals in the US and China in terms of their avoidance of online security threats.	Avoidance (a coping behaviour that safeguards against the online security threat by not using the Internet)	PMT, TTAT	Survey	In both China and the US, individuals' avoidance was positively influenced by threat perception but negatively influenced by self-efficacy.
Lowry and Moody (2015)	Studied the reactance response of employees to a new organisational ISec policy by using an approach that combined control theory and reactance theory	Reactance	Control theory; reactance theory	Experiment	The employees' strong reactance response was not conducive to their intent of new ISec policy compliance.
D'Arcy, Herath, and Shoss (2014)	Studied the EFC of employees to stressful ISec requirements based on moral disengagement theory (MDT)	Mental relaxation; modify work tasks; reinvent the technology	Coping theory; MDT	Survey	EFC encouraged the ISec policy violation intention of employees.
Chenoweth, Minch, and Gattiker (2009)	Studied the role of individual users' avoidance of using anti-spyware in a PMT-based model	Avoidance	PMT	Survey	Individuals with a higher tendency to avoidance were influenced by a higher response cost perception and had weaker protection motivation.

obscure or distort, and (iii) devalue the target. These three response categories are moral disengagement mechanisms in moral disengagement theory (MDT). According to D'Arcy, Herath, and Shoss (2014, 292), these responses can be regarded as EFC because 'there is conceptual overlap between the general descriptions of emotion-focused coping in the stress literature and the mechanisms of moral disengagement as articulated in MDT.' However, the moral disengagement mechanisms studied by D'Arcy, Herath, and Shoss (2014) are difficult to label as EFC. As mentioned in Section 2.1, EFC is a response to a stressor, threat, or challenge with the goal of regulating emotions. MDT is used to explain why some people can perform inhumane/destructive behaviours without exhibiting distress (Bandura 1999, 2002). According to MDT, moral disengagement mechanisms are used to reconstruct destructive behaviour in order to make them morally acceptable. Therefore, these mechanisms should not be confused with EFC strategies.

Finally, previous ISec studies have focused on only a few EFC strategies. However, other coping strategies may be relevant in contexts of electronic device abuse and ISec policy violations. Accordingly, the roles of other EFC strategies and the differences between them need to be explored and empirically examined. Liang and Xue (2009) called for the following work on EFC:

> We propose that users can take both problem- and emotion-focused coping to reduce IT threats. In the IT threat context, emotion-focused coping cannot be overlooked, and the interaction between the two coping strategies leads to some interesting relationships that have important implications for IS research and practice. (86)

Liang and Xue (2010, 405) further emphasised the need to investigate the conditions that lead to EFC and its influence on PFC. In a recent study, Liang et al. (2019) divided EFC strategies into inward and outward, showing that they had completely different effects on PFC. They emphasised the importance of EFC and called for further research to confirm relevant EFC strategies in different IT security contexts (390). However, Liang et al. (2019) regarded three different inward EFC strategies as components of inward EFC but did not study the subtleties of each strategy. However, different inward EFC strategies may induce the same risk ISec behaviour. Investigating their characteristics and effects may help in understanding the reasons for individuals' ISec behaviours. In the present study, we contribute to this gap in the research by focusing on the inward EFC strategies (e.g. fatalism and hopelessness) noted by Liang and Xue (2009, 78). Next, we describe the coping strategies and theories that form the framework of our study.

3. Theoretical framework of the study

While this study primarily focuses on EFC and coping theory, the research model is based on PMT. PMT is derived from coping theory, but it provides details that explain individuals' cognitive processes in responding to threats. We further explain these cognitive processes and the subsequent effects of individuals' inward EFC.

3.1. EFC in coping theory and PMT

Coping theory describes coping processes[3] in managing psychological stress, thus providing a theoretical framework for understanding how an individual responds to a stressor. Two processes mediate the relationship between the person and the stressor (environment): appraisal and coping. Appraisal is a cognitive process through which an individual evaluates perceived stress (i.e. primary appraisal) and assesses available coping resources (i.e. secondary appraisal). Although individuals consider how to cope with stress only after they perceive it, Lazarus and Folkman (1984) emphasised that primary and secondary appraisals do not occur in a linear sequence. On the contrary, primary and secondary appraisals may cycle repeatedly in a transaction, often operating in harmony. Furthermore, the outcome of one appraisal process may trigger a reassessment of the former. The combination of primary and secondary appraisals has been shown to result in coping efforts aimed at reducing stress (Lazarus and Folkman 1984; Folkman et al. 1986). As described in section 2.1, the two main functions of coping efforts include PFC, which manages stressors, and EFC, which regulates the emotions caused by stress (Folkman and Lazarus 1980; Lazarus and Folkman 1984).

Although PMT originated in coping theory, it elaborates the cognitive process and its effect on the coping intention of an individual (Rogers 1975, 1983). PMT includes two cognitive processes: threat appraisal and coping appraisal (Rogers 1975, 1983). The threat appraisal process is related to an individual's perception of how threatened they feel (i.e. primary appraisal). The coping appraisal process involves an assessment of an individual's ability to cope with the threat (i.e. secondary appraisal). The combination of threat and coping appraisals intervenes in the individual's protection motivation, which refers to the intention[4] to initiate, continue, or inhibit the applicable adaptive responses. Similar to Lazarus's coping theory (1984), protection motivation can be explained as the behavioural intention to cope with the threat in an adaptive way (i.e. PFC). Although the original PMT did not include

EFC, it gradually received attention after Rippetoe and Rogers (1987) study. This point is noteworthy because the 'full nomology' of Boss et al. (2015) is silent on this issue. Rippetoe and Rogers (1987) used PMT as the theoretical background to conduct an empirical study on five different EFC strategies (i.e. avoidance, religious faith, fatalism, wishful thinking, and hopelessness) for coping with breast cancer. The five EFC strategies were offered by McCrae (1984), who identified several distinct coping mechanisms based on Lazarus's coping theory. Subsequently, Rogers, Prentice-Dunn, and Gochman (1997) and Milne, Sheeran, and Orbell (2000) included EFC as another coping mode in their PMT review studies.

3.2. Inward EFC strategies

Based on Liang et al. (2019) classification of EFC (i.e. inward vs. outward), in this study, we focus on inward EFC strategies because they impede individuals in performing PFC. According to Liang et al. (2019), outward EFC refers to the direct adjustment of emotional responses generated. Individuals regulate the physiological and experiential aspects of emotions through communication or other approaches, thereby reducing the negative effects of emotions, such as emotional support seeking. Inward EFC refers to the prevention of negative emotions by shifting or distracting attention or distorting the perception or appraisal of threats, such as denial. It involves 'approaches internal to the self and unobservable to others' (Liang et al. 2019, 377). According to Liang et al. (2019), although the goal of both inward and outward EFC is to restore the emotional stability of individuals, they achieve it differently. Outward EFC alleviates the negative effects of stressors or emotions by directly regulating the emotions generated by threats, but it does not deliberately change the perception of the threats. Therefore, outward EFC can promote rational responses such as PFC. Inward EFC prevents the appearance of negative emotions by ignoring or distorting the perception or appraisal of threats, such as by denying their existence. This response hinders PFC responses, thereby increasing the possibility that the individual will engage in risky behaviour.

We chose to test five inward EFC strategies (i.e. avoidance, reactance, wishful thinking, hopelessness, and fatalism) that individuals often use when they face threats (Folkman and Lazarus 1985; McCrae and Costa 1986; Rippetoe and Rogers 1987), which are also concerns in ISec research (Liang and Xue 2009).

3.2.1. Avoidance (denial)

Avoidance is the motivated resistance to actively evade, minimise, or even deny a threat (Rippetoe and Rogers 1987; Witte 1992), which is also known as denial in the coping literature. For example, users who reuse passwords may deliberately deny that this behaviour may lead to the risk of multiple accounts being stolen. In the PMT framework, avoidance plays the role of reducing fear but simultaneously weakens intentions to adopt an adaptive response (Abraham et al. 1994; Chenoweth, Minch, and Gattiker 2009). Avoidance can be aroused by high threat information or fear but reduced if information about adaptive coping responses is provided (i.e. high response efficacy) or the individual has high self-efficacy perception (Rippetoe and Rogers 1987; Witte 1991; Eppright et al. 2003; Fry and Prentice-Dunn 2005b, 2005a).

Avoidance also exists as a PFC strategy in other respects. In IS, Liang and Xue (2009, 2010) developed the TTAT, which explains the behaviour of individual users in avoiding malicious IT threats. In this context, avoidance means avoiding malicious IT threats by taking safeguarding measures. These actions are a form of PFC, but they are often confused with an EFC response. In addition, studies in the field of cognitive and developmental psychology have suggested that when people must deal with highly stressful and unchangeable events, such as cancer, avoidance is an alternative adaptive strategy and a self-defence mechanism (Cramer 2000; Seiffge-Krenke 2004). In such cases, avoidance may be associated with positive outcomes in the short term, but the positive effects will diminish over time (Kazak and Meadows 1989).

3.2.2. Reactance

Reactance refers to an individual's reaction to the perceived lack of self-determination by (re)asserting control when they feel they are being externally controlled or their freedom is being reduced (Witte 1992; Lowry and Moody 2015). For example, a user may oppose updating the mobile operating system (OS) by thinking that this behaviour will affect their freedom in using a mobile phone. According to psychological reactance theory, reactance is a negative emotional response to threats or external resources, which is motivated by the human need for self-determination. Although, like avoidance, reactance is maladaptive behaviour, unlike avoidance, reactance is an active negative response in the attempt to challenge the causes of negative emotions rather than lower the emotions themselves (J. W. Brehm 1966; S. S. Brehm and Brehm 1981; Burgoon et al. 2002). To date, reactance has received little empirical interest in the ISec field. Lowry and Moody (2015) used reactance theory to explain the motivation of employees for non-compliance with a new ISec policy. They found that the threat to employees' freedom in self-expression increased their reactance to the new ISec policy, and the resulting reactance decreased their intention to comply with it. Furthermore, Witte and Allen (2000) conducted a meta-analysis and found that persuasive messages of high threat and low efficiency produced the greatest reactance and avoidance in the healthcare field.

3.2.3. Wishful thinking

Wishful thinking is an EFC strategy that 'prompts the use of panaceas or unrealistic solutions to a problem' (Rippetoe and Rogers 1987, 598). This strategy is related to avoidance, but it reduces or eliminates negative emotions the resort to fantasy (Livneh 2000). Individuals who engage in wishful thinking construct relevant beliefs based on their desire rather than on reality (Liang et al. 2019). The response of wishful thinking can concern different objects. For example, some users unrealistically believe that the mobile phone protection system can prevent malware attacks. In PMT, a high threat appraisal associated with a low response appraisal was found to produce a greater amount of coping by wishful thinking (Rippetoe and Rogers 1987; Self and Rogers 1990).

3.2.4. Hopelessness and fatalism

Fatalism refers to an individual's acceptance of the situation as unavoidable or 'fate' because 'nothing can be done anyway' (Rippetoe and Rogers 1987, 598). Hopelessness is defined as the lack of belief in possible solutions to threats (McCrae and Costa 1986; Rippetoe and Rogers 1987). Hopelessness and fatalism are two phenomena in behavioural disengagement; that is, individuals reduce or even give up efforts or attempts to deal with threats or stressors (Carver, Scheier, and Weintraub 1989). They are considered passive compared with other EFC strategies (Livneh 2000). However, the main difference between hopelessness and fatalism is that fatalism is in response to acceptance of the situation, whereas the response of hopelessness indicates non-acceptance of the situation. Furthermore, hopelessness is more likely to lead to counterproductive behaviour, such as abandoning oneself to despair or giving up on avoiding danger (Rippetoe and Rogers 1987). Previous studies showed that individuals with high threat perception and low response efficacy tended to demonstrate more hopelessness and fatalism (Fruin, Pratt, and Owen 1992; Prentice-Dunn, Floyd, and Flournoy 2001).

The above five EFC strategies involve approaches that are unobservable and internal to the self, serving to maintain emotional stability in the short term by ignoring or diverting attention away from threats or distorting the perception of threats. These EFC strategies have been shown to impede adaptive coping or PFC (Chenoweth, Minch, and Gattiker 2009; Lowry and Moody 2015; Liang et al. 2019). Therefore, we consider that the five strategies are considered inward EFC strategies. Table 3 shows their operational definitions in the context of mobile malware threats in this study.

Table 3. Operational Definitions of Inward EFC Strategies.

Construct	Definition	Source
Avoidance (denial)	An individual user's attempt to actively evade or deny the mobile malware threat.	Rippetoe and Rogers (1987); Carver, Scheier, and Weintraub (1989)
Reactance	An individual user who perceives that their freedom is being reduced because of the need to take action to protect their mobile phone information security and who is likely to react to that perceived lack of self-determination by (re)asserting control.	Lowry and Moody (2015); Witte (1992)
Hopelessness	An individual user's absence of belief in possible solutions to the mobile malware threat without acceptance.	Rippetoe and Rogers (1987); Carver, Scheier, and Weintraub (1989)
Wishful thinking	An individual user's attempt to wish that the mobile malware threat would disappear or use unrealistic solutions to the mobile malware threat.	Rippetoe and Rogers (1987); McCrae and Costa (1986)
Fatalism	An individual user's acceptance of the mobile malware threat as unavoidable, unchangeable, or 'fate.'	Rippetoe and Rogers (1987); McCrae and Costa (1986)

4. Research model and hypotheses

4.1. Definitions and hypotheses of constructions in the PMT core framework

Following Milne, Sheeran, and Orbell (2000) schematic representation of PMT, we placed the five EFC strategies within the PMT framework (Figure 2). Based on PMT, we propose that an individual's behaviour to protect mobile phone ISec can be determined by the corresponding protection motivation. Moreover, the protection motivation is influenced by the individuals' cognitive assessment of ISec threats,[5] which is the mobile malware in this study (Rogers 1983; Rogers, Prentice-Dunn, and Gochman 1997).

As described above, there are two main cognitive mediating processes: threat appraisal and coping appraisal. In this study, threat appraisal refers to the process of evaluating an individual's perception of how dangerous mobile malware is if no action were taken. The factors comprising threat appraisal are threat severity and threat vulnerability. Threat severity is

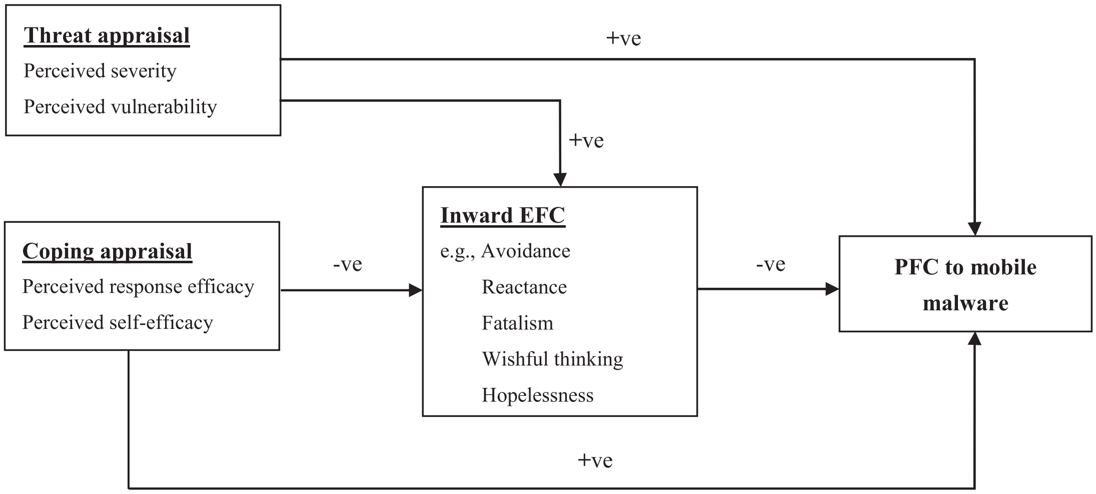

Figure 2. Research model (adapted from Milne, Sheeran, and Orbell (2000)). +ve = positive association; -ve = negative association.

defined as an individual's belief about the magnitude of the negative consequences of a mobile malware threat. Threat vulnerability is defined as an individual's belief about the possibility of experiencing a mobile malware threat. Following Lazarus and Folkman (1984) and Rogers (1983), in this study, we defined PFC intention as the motivation for individual users to deal directly with mobile malware threats. In this study, it refers to the PFC intention to update the mobile's OS in a timely manner. Previous research on information behaviour provided theoretical and empirical evidence that perceived severity and probability of ISec threats motivate individuals to take protective measures (Boss et al. 2015; Chen and Zahedi 2016). However, a considerable number of ISec studies have shown inconsistent results regarding this conclusion. For example, perceived threat severity or vulnerability in some studies did not predict individuals' PFC intentions (Woon, Tan, and Low 2005; Ng, Kankanhalli, and Xu 2009; Crossler and Bélanger 2014; Johnston, Warkentin, and Siponen 2015). Despite these conflicting results, we will test the following hypotheses in the mobile malware context:

> H1a: The perceived severity of mobile malware positively affects the PFC intention of individual users.

> H1b: The perceived vulnerability of mobile malware positively affects the PFC intention of individual users.

The term coping appraisal refers to the process of evaluating an individual's ability to 'cope with or avert the threatened danger' (Floyd, Prentice-Dunn, and Rogers 2000, 410). It considers two main factors: response efficacy and self-efficacy. Response efficacy is defined as an individual's belief that the recommended coping responses will effectively protect the mobile's information security. Self-efficacy is defined as an individual's belief that they have the ability to perform the recommended response. Previous ISec studies have consistently shown that the perceived effectiveness of protective measures and high self-efficacy could motivate individuals to perform PFC behaviours (Johnston and Warkentin 2010; Boss et al. 2015; Chen and Zahedi 2016). Based on the theoretical and empirical evidence, we propose the following hypotheses:

> H2a: Response efficacy positively affects the PFC intention of individual users.

> H2b: Self-efficacy positively affects the PFC intention of individual users.

4.2. Hypotheses regarding inward EFC strategies

In this study, inward EFC refers to behavioural responses aimed at reducing emotional distress by shifting or distracting attention from or distorting perception, rather than directly managing mobile malware threats (Rogers, Prentice-Dunn, and Gochman 1997; Liang et al. 2019). A high level of threat perception invokes both EFC and PFC (Rippetoe and Rogers 1987; Prentice-Dunn, Floyd, and Flournoy 2001; Eppright et al. 2003), but it may prompt inward EFC in the absence of a high coping appraisal (Witte 1991; Ruiter, Abraham, and Kok 2001). This conclusion was drawn in the physiological and mental health fields and subsequently confirmed by Liang et al. (2019) and Chen and Zahedi (2016), but it has not been universally accepted in other ISec research. A simple example based on this conclusion is the following: when individual users perceive an overwhelming mobile malware threat, they may have unrealistic hopes that the threat will disappear. Therefore, we hypothesise the following:

H3a: The perceived severity of mobile malware positively affects the inward EFC of individual users.

H3b: The perceived vulnerability of mobile malware positively affects the inward EFC of individual users.

An individual's evaluation of their response efficacy and self-efficacy is the key factor in determining whether it results in an EFC or a PFC response (Witte 1991, 1996; Witte and Allen 2000). Many studies on cancer threats have indicated that response efficacy plays a role in decreasing individuals' EFC response to cancer (Prentice-Dunn, Floyd, and Flournoy 2001; Eppright et al. 2003; Fry and Prentice-Dunn 2005b, 2005a). Rippetoe and Rogers (1987, 596) concluded that 'high response efficacy and high-self-efficacy conditions did not foster any maladaptive coping.' Regarding the theoretical level of ISec, Liang and Xue (2009) stated that safeguarding effectiveness and self-efficacy helped reduce EFC to malicious IT threats. For example, if individual users had negative beliefs about the corresponding measures or their ability to implement these measures, then they were likely to feel helpless or deny the ISec threat instead of taking any effective measures. However, Chen and Zahedi (2016) demonstrated that perceived self-efficacy negatively affected individuals' intention to avoid using the network. The relationship between coping appraisal and inward EFC requires empirical examination. Therefore, we need to further evaluate the relationship between coping appraisal and inward EFC:

H4a: Response efficacy negatively affects the inward EFC of the individual user.

H4b: Self-efficacy negatively affects the inward EFC of the individual user.

The health psychology literature shows different outcomes of the relationship between individuals' EFC and PFC. On one hand, previous health studies on AIDS found that avoidance (i.e. denial) was more likely to undermine precaution motivation (Van der Velde and Van der Pligt 1991; Abraham et al. 1994). On the other hand, inward EFC failed to predict AIDS-related PFC responses (Umeh 2004). However, regarding IS threats, inward EFC has been shown to decrease the PFC response of individuals. In the context of an organisation's ISec policy compliance, Lowry and Moody (2015) found that reactance to a new ISec policy negatively affected the compliance intention of employees. In the context of individuals' behaviour, Chenoweth, Minch, and Gattiker (2009) found a passive effect on individuals' EFC strategies regarding their intention to adopt IT protection technologies. In our context, if individual users had already accepted that the mobile malware threat was unavoidable, then they may have lost the intention to engage in behaviour to protect ISec. In line with the existing research, we propose the following hypothesis:

H5: Inward EFC strategies negatively affect the PFC intention of individual users.

In addition, we evaluated the effects of six control variables in the research model: age, gender, mobile OS, previous experience using mobile phones, importance of the information stored on the mobile phone, and previous exposure to a similar ISec threat. These control variables are discussed in Appendix D.

5. Research methodology

To evaluate the research model, we conducted a survey with a sample of staff members and students at a university in China. Mobile malware was the ISec threat, and the timely updating of the mobile phone's OS represented one of the most effective adaptive responses against mobile malware threats (Security and Report 2018). Thus, in this study, protection intention involved individuals in updating the OSs of their mobile phones in a timely manner.

5.1. Measurement development

Ten constructs were measured in this study: PFC, threat severity, threat vulnerability, response efficacy, self-efficacy, and five inward EFC strategies (i.e. avoidance, reactance, wishful thinking, hopelessness, and fatalism). We developed the items in the multi-item scales based on the theoretical meaning of the constructs and the original literature (Rippetoe and Rogers 1987; Witte 1992, 1996; Milne, Orbell, and Sheeran 2002; Eppright et al. 2003). These items have been validated multiple times and adapted to the mobile malware context. To ensure content validity, in addition to the literature review, we performed a pre-test, a questionnaire translation procedure, and a pilot test. Appendices B1 and B2 provide detailed information about the survey items and the validation process conducted to ensure content validity.

5.2. Data collection

In this study, four hundred and forty-six students and staff members at a major university in China were selected as the research subjects. Because they accounted for a considerable proportion of the smartphone user group, they could appropriately represent individual smartphone users. Participants were asked to complete the anonymous questionnaire online by their phones with the supervisor's help. A total of 421 students and staff members completed the survey, which was a response rate of 94.4%. To ensure the validity of the responses, we cleaned the data as follows: 1) adding bogus items to the questionnaire; and 2) removing all observations completed in less than three minutes. The reason was that the pilot test indicated that at least three minutes were needed to answer the questionnaire carefully (Meade and Craig 2012). We also set up the online survey so that there were no missing values in the responses. The final data set included 406 usable observations. The sample size satisfied the rule of thumb required in structural equation modelling (Kline 2011). The demographic statistics of the sample are reported in Appendix A.

5.3. Data analysis and results

We used STATA version 15.1 to check the reliability and validity of the instrument and test the hypotheses.

5.3.1. Instrument validity

We conducted a confirmatory factor analysis to check the convergent and discriminant validities of the measurement. The factor loadings for the items in the measurement model were in excess of 0.707, and the corresponding z-value was significant (Appendix B.3) (Gefen, Straub, and Boudreau 2000; Straub, Boudreau, and Gefen 2004). The principle factor analysis showed that all items loaded on the posited construct at 0.49 or greater (Appendix B.4) (Hair et al. 1998). Therefore, these results supported the convergent validity of all constructs in the survey. Discriminant validity is established if each item in the same construct has a higher loading than the other constructs (Straub, Boudreau, and Gefen 2004), and the square root of each construct's average variance extracted (AVE) is higher than its correlations with other constructs (Fornell and Larcker 1981). Thus, our results also supported the discriminant validity. In addition, the fit index of the measurement model also met the requirements for good discriminant and convergent validities (Straub, Boudreau, and Gefen 2004) (Table 4).

In addition to verifying adequate validity, our measurement presented high reliability. Table 5 shows the results of the construct reliability checks. The Cronbach's alpha values of all constructs were above 0.80, which exceeded the threshold of 0.70 (Nunnally, Bernstein, and Berge 1978). The composite reliability scores exceeded the cut-off value of 0.70 (Fornell and Larcker 1981; Gefen and Straub 2005). Therefore, measurement reliability was proven to be adequate.

Table 4. Model Statistics and Fit Indices.

Fit index	Measurement model	Theoretical model
χ2	827.66	1312.44
Df	494	738
Normed χ2	1.675	1.778
CFI (Comparative Fit Index)	0.969	0.947
TLI (Tucker–Lewis Index)	0.963	0.937
Root mean square error of approximation	0.041	0.044
Standardised root mean square residual	0.031	0.066

Table 5. Reliability Checks.

Constructs	Cronbach's alpha	Composite reliability	AVE
Threat severity	0.819	0.770	0.529
Threat vulnerability	0.883	0.865	0.681
Response efficacy	0.894	0.851	0.656
Self-efficacy	0.908	0.893	0.736
PFC intention	0.928	0.912	0.776
Avoidance	0.897	0.880	0.709
Reactance	0.917	0.883	0.791
Hopelessness	0.935	0.904	0.759
Fatalism	0.885	0.855	0.665
Wishful thinking	0.838	0.792	0.560
Important information on the mobile	0.930	0.919	0.790
Previous exposure to Similar ISec threat	0.962	0.957	0.882

Note: AVE = average variance extracted

5.3.2. Common method bias

All the constructs of the study were measured through the participants' self-reports, leading to possible common method variance (CMV). We took procedural and statistical steps to control method biases. We ensured that each item was concise and straightforward in the process of verifying the content validity by avoiding unfamiliar terms and vague concepts (Tourangeau, Rips, and Rasinski 2000). The anonymity of the participants was protected to reduce social desirability bias. Moreover, the order of measurement of the independent variables and the dependent variable was balanced to control biases related to the items' embeddedness (Tehseen, Ramayah, and Sajilan 2017). In terms of statistics, no large correlations were found (r <0.9) among all constructs according to the correlation matrix of latent variables (Table 6) (Bagozzi, Yi, and Phillips 1991). We also evaluated the model using Harman's one-factor test (Podsakoff et al. 2003). After the exploratory factor analysis without factor rotation, the eigenvalues of nine factors were greater than 1, which explained 95.99% of the data variance. The data variance explained by the first factor was only 27.66%, accounting for 28.82% of the total variance, which did not exceed the 25–50% range required by Hair et al. (1998). The results indicated that CMV was not a serious problem in these data.

Table 6. Correlations, AVE, Means, and Standard Deviations of Constructs.

Constructs	Mean	Std	1	2	3	4	5	6	7	8	9	10	11	12
Threat severity	5.74	0.06	**0.727**											
Threat vulnerability	4.70	0.07	0.33	**0.825**										
Response efficacy	4.95	0.07	0.20	0.12	**0.810**									
Self-efficacy	5.30	0.07	0.12	0.02	0.38	**0.858**								
PFC intention	4.14	0.08	0.13	0.13	0.47	0.42	**0.881**							
Avoidance	4.09	0.08	−0.23	−0.09	−0.06	−0.07	−0.19	**0.842**						
Hopelessness	3.02	0.07	−0.10	0.03	−0.47	−0.23	−0.26	0.21	**0.871**					
Wishful thinking	2.74	0.06	−0.11	−0.16	−0.13	−0.03	−0.12	0.22	0.36	**0.748**				
Reactance	3.01	0.07	−0.27	−0.12	−0.21	−0.14	−0.10	0.24	0.35	0.35	**0.889**			
Fatalism	3.27	0.08	0.08	0.12	−0.14	−0.08	−0.19	0.28	0.32	0.32	0.17	**0.816**		
Previous exposure to similar ISec threat	3.17	0.09	0.11	0.24	−0.01	0.02	0.10	−0.08	0.05	0.02	−0.04	0.08	**0.939**	
Important information on the mobile	6.05	0.06	0.39	0.19	0.12	0.16	0.16	−0.10	−0.16	−0.17	−0.21	−0.04	0.05	**0.889**

Note. The diagonal elements represent the square roots of average variance extracted (AVE).

5.3.3. Model testing

We estimated the structural equation model by using the maximum likelihood method and testing the theoretical model based on the research model described above. Figure 3 shows the estimation results. All the fit indices of the theoretical model reached the cut-off threshold proposed by Hooper, Coughlan, and Mullen (2008), indicating that the theoretical model was acceptable.

As shown in Table 7 and Figure 3, the best model accounted for 8% of the variance in avoidance, 16% of the variance in reactance, 30% of the variance in hopelessness, 7% of the variance in fatalism, 7% of the variance in wishful thinking, and 40% of the variance in protection intention. The R-squared values of the endogenous variables were statistically significant (Figure 3), indicating the reasonable explanatory power of the model. As hypothesised, the results of the structural model analysis partially supported the relationship between the main factors of PMT; that is, response efficiency (β = 0.427, $p = 0.000$) and self-efficacy (β = 0.298, $p = 0.000$) had significant positive effects on the PFC intention of individual users. Similarly, H3b, H4a, and H5 were partially supported. Threat vulnerability had a significant positive effect on fatalism (β = 0.173, $p = 0.007$) and hopelessness (β = 0.122, $p = 0.009$) but a marginally significant negative effect on wishful thinking (β = −0.096, $p = 0.052$), but

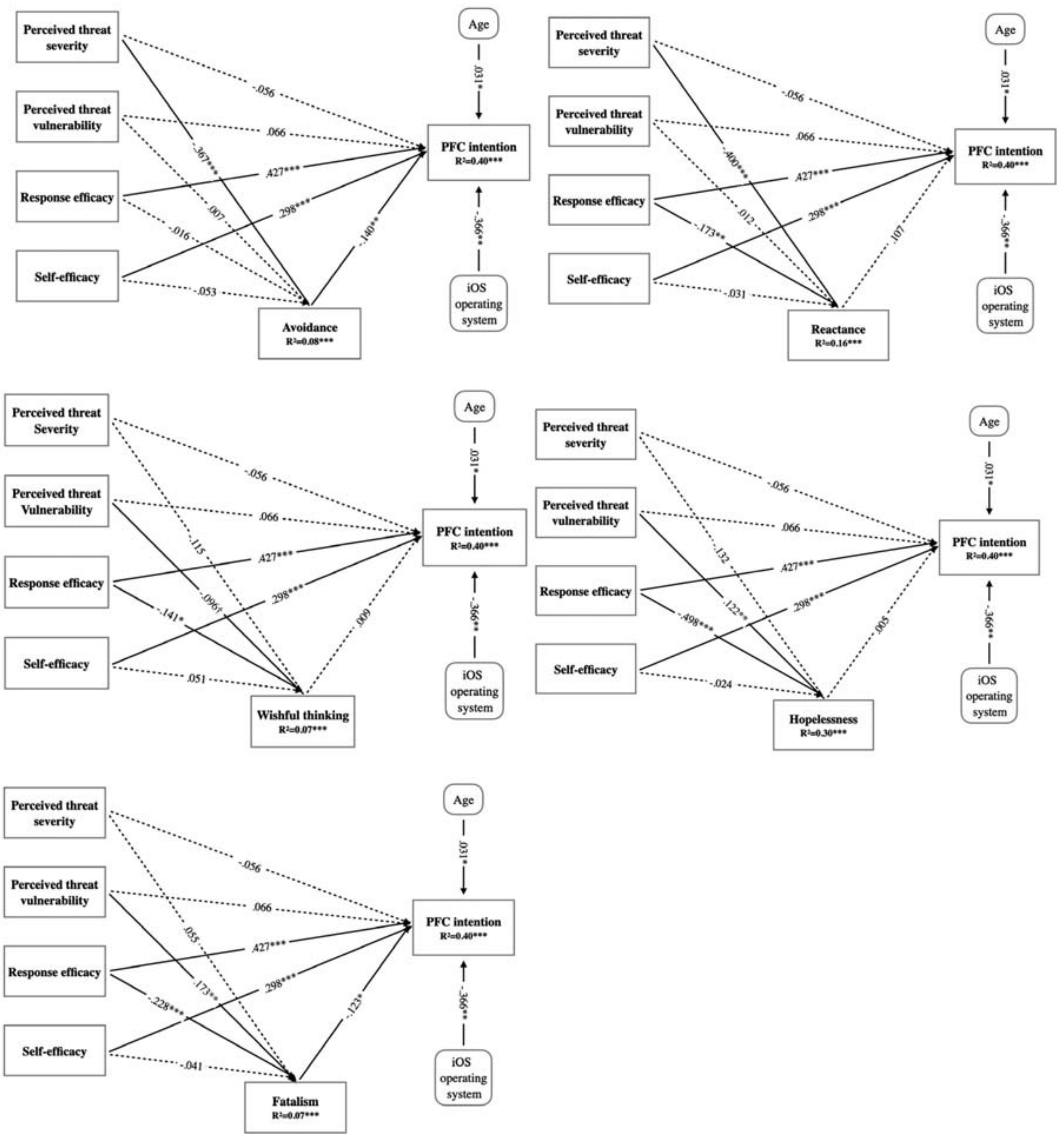

Figure 3. Model test results.

Table 7. Hypothesis Verification Results.

Hypotheses	Path	Path coefficient	Supported
H1a: The perceived severity of mobile malware positively affects the PFC intention of individual users.	Threat Severity → Intention	−0.056(n/s)	No
H1b: The perceived vulnerability of mobile malware positively affects the PFC intention of individual users.	Threat Vulnerability → Intention	0.066(n/s)	No
H2a: Response efficacy positively affects the PFC intention of individual users.	Response efficacy → Intention	0.427***	Yes
H2b: Self-efficacy positively affects the PFC intention of individual users.	Self-efficacy → Intention	0.298***	Yes
H3a: The perceived severity of mobile malware positively affects the inward EFC of individual users.	Threat Severity → Avoidance	−0.367***	No
	Threat Severity → Reactance	−0.400***	No
	Threat Severity → Fatalism	0.055(n/s)	No
	Threat Severity → Hopelessness	−0.132(n/s)	No
	Threat Severity → Wishful thinking	−0.115(n/s)	No
H3b: The perceived vulnerability of mobile malware positively affects the inward EFC of individual users.	Threat Vulnerability → Avoidance	0.007(n/s)	No
	Threat Vulnerability → Reactance	0.012(n/s)	No
	Threat Vulnerability → Fatalism	0.173**	Yes
	Threat Vulnerability → Hopelessness	0.122**	Yes
	Threat Vulnerability →Wishful thinking	−0.096(†)	No
H4a: Response efficacy negatively affects the inward EFC of individual users.	Response efficacy → Avoidance	−0.016(n/s)	No
	Response efficacy → Reactance	−0.173**	Yes
	Response efficacy → Fatalism	−0.228**	Yes
	Response efficacy → Hopelessness	−0.498***	Yes
	Response efficacy → Wishful thinking	−0.141*	Yes
H4b: Self-efficacy negatively affects the inward EFC of individual users.	Self-efficacy → Avoidance	−0.053(n/s)	No
	Self-efficacy → Reactance	−0.031(n/s)	No
	Self-efficacy → Fatalism	−0.041(n/s)	No
	Self-efficacy → Hopelessness	−0.024(n/s)	No
	Self-efficacy → Wishful thinking	0.051(n/s)	No
H5: Inward EFC strategies negatively affect the PFC intention of individual users.	Avoidance → PFC intention	−0.140**	Yes
	Reactance → PFC intention	0.107(n/s)	No
	Fatalism → PFC intention	−0.123*	Yes
	Hopelessness → PFC intention	0.005(n/s)	No
	Wishful thinking → PFC intention	0.009(n/s)	No

Note. *$p \leq 0.05$, **$p \leq 0.01$, ***$p \leq 0.001$, $^{\dagger}0.05 \leq p \leq 0.1$, n/s refers to insignificant.

it did not significantly affect reactance and avoidance. Response efficacy had a significant negative impact on the four other inward EFC strategies in addition to avoidance. Avoidance ($\beta = -0.140$, $p = 0.01$) and fatalism ($\beta = -0.123$, $p = 0.013$) had significant negative effects on the protection intention of individual users. However, reactance, wishful thinking, and hopelessness did not affect protection intention. The results did not support H3a and H4b. Specifically, perceived threat severity did not have a significant positive effect on inward EFC strategies. Conversely, it had significant negative effects on avoidance, reactance, and hopelessness. Self-efficacy did not have a significant negative effect on any inward EFC strategy.

In addition, two control variables (i.e. age and mobile OS) significantly affected the PFC of individual users. These results are shown and discussed in Appendix D.

5.3.4. Effects of participants' backgrounds on inward EFC strategies

Using ANOVA and a regression analysis, we analysed the effects of the participants' backgrounds on their preference for a specific inward EFC strategy. Interestingly, overall, the participants did not have a strong willingness to adopt inward EFC strategies. The means of each inward EFC strategy in each background did not exceed 4.6. Among the five inward EFC strategies, avoidance was the strategy favoured by the participants. Regarding age, compared with the other age groups, the age group 35–46 years was more inclined to choose hopelessness when they faced mobile malware threats (p <0.05). The participants in the age group 25–34 years were more inclined to wishful thinking (p <0.05). Coincidentally, the results for the participants' professional backgrounds were consistent with the results for their age backgrounds. Compared with the students, the university staff members preferred wishful thinking and hopelessness when they faced mobile malware threats. The potential reason for this finding is the high correlation between age and profession. Moreover, participants with less than one year of smartphone use experience (p <0.05) or who used iOS (p<0.05) preferred to adopt wishful thinking when they were faced with malware threats. Finally, the more critical the data and information stored in the mobile phone, the more that participants avoided adopting inward EFC strategies, with the exception of fatalism. Further details and explanations regarding these results are provided in Appendix E.

6. Discussion

6.1. Key findings

This study evaluated conceptual differences among five inward EFC strategies based on coping theory and PMT. It also empirically analysed the effects of these inward EFC strategies on individual users' PFC responses and the role of cognitive factors in their responses. The empirical results partially supported hypotheses H2, H3b, H4a, and H5. The results showed that avoidance and fatalism significantly impeded individual users' PFC responses to mobile malware threats. These users did not practice PFC because they ignored or denied the existence of mobile malware, or they believed that the malware was unavoidable, and they passively accepted the situation. The obstructive effect of avoidance on PFC has been shown in previous studies by Chenoweth, Minch, and Gattiker (2009) and Liang et al. (2019) in the ISec research field. However, the effect of fatalism on PFC is a new finding in this area. This result aligns with PMT and previous findings in the health psychology literature (Rippetoe and Rogers 1987; Van der Velde and Van der Pligt 1991; Abraham et al. 1994; Chenoweth, Minch, and Gattiker 2009). Rippetoe and Rogers (1987) suggested that fatalism might be one of the most inward EFC mechanisms because individuals had accepted their predicament and hence ceased to engage in any other form of coping. However, if individual users believed that ways to counter mobile malware threats were helpful, they were more likely to adopt a PFC response than an inward EFC strategy. Based on these results, response efficiency had a significant negative effect on inward EFC strategies but a positive effect on PFC (H2a and H4a).

In this study, H3 was partially confirmed. The findings suggested that perceived threat vulnerability positively affected individual users' adoption of hopelessness and fatalism but not of other inward EFC strategies. That is, if individual users perceived that a mobile malware attack was highly likely or that it was unavoidable, they were more likely to stop responding to the threat because the 'facts' could not be changed. This result confirmed differences between inward EFC strategies. Based on our conceptual clarification of five inward EFC strategies in the literature review and the empirical results of this study, we concluded that inward EFC strategies can be categorised as either active or passive. Individuals who adopted passive inward EFC strategies (i.e. hopelessness and fatalism) considered the situation or problem inevitable (i.e. high threat vulnerability perception), and they lacked faith in a solution (i.e. low response efficacy perception). They showed reductions in or the abandonment of hope or the willingness to respond to threats (Rippetoe and Rogers 1987; Carver, Scheier, and Weintraub 1989; Livneh 2000), which was unfavourable to the PFC response. In contrast, individuals who adopted active EFC strategies (i.e. avoidance, reactance, and wishful thinking) proactively ignored, denied, or distorted facts, such as through cognitive efforts, and they were more inclined not to accept the existence of threats. Thus, adoption may be weakly related to threat vulnerability.

However, H3 was only partially supported. The results showed that the severity of the perception of mobile malware threats was negatively associated with the individual's willingness to adopt avoidance and reactance. Threat vulnerability perception was slightly significantly negatively associated with wishful thinking. However, it is possible that these interesting findings could indicate the complex psychological responses of individual users in the context of malware threats. Because individuals' evaluations of the outcomes of different coping mechanisms are contextual, a specific situation may shape the inward EFC strategy adopted by individual users, such as the type or technological attributes of ISec threats (Liang et al. 2019).

This study was conducted in the mobile malware context. Because smartphones have been commercially available for decades, users may believe that the security features of these devices block most cyberattacks, which causes them to relax their vigilance regarding malware threats. Moreover, malware threats are not new, and their repeated exposure may also desensitise users. Therefore, users may have a lower-than-expected threat appraisal of malware threats. If an individual believes that the consequences of a threat are not severe, even if PFC were not adopted, they may employ inward EFC strategies that are less demanding, such as ignoring a threat or distorting the threat perception. In contrast, wishful thinking has been considered conceptually similar to unrealistic optimism (Liang et al. 2019). Individuals who are unrealistically optimistic usually have the mistaken belief that their chances of encountering negative events or threats are lower than those of others. This reaction is in response to the reluctance to accept their vulnerability to the threat (Weinstein 1980, 1982), which could be the reason that wishful thinking was shown to be negatively related to the perceived threat vulnerability of individuals (McMath and Prentice-Dunn 2005).

Finally, hypotheses H1, H3a, and H4b have not been examined in the ISec field. Our findings showed that individual users' self-efficacy did not significantly affect inward EFC in our context, and hopelessness, reactance, and wishful thinking may not have affected individuals' intention to protect their mobile ISec. These findings are consistent with those of previous health psychology studies (Eppright et al. 2003; Umeh 2004; Fry and Prentice-Dunn 2005b; Chenoweth, Minch, and Gattiker 2009). Based on our findings, the role of inward EFC strategies in response to ISec threats in the PMT framework may change because of individual differences, stressors, cultural factors, or environmental factors (Lazarus and Folkman 1984; Carver, Scheier, and Weintraub 1989; Chen and Zahedi 2016). In the present study, the unclear association found between reactance and PFC was reasonable because the target population consisted of individual users. Unlike mandatory ISec policies in organisations, which may cause individuals to perceive a lack of self-determination, individual users have autonomy in using their smartphones, so they may not demonstrate stronger reactance coping intentions than in organisational contexts.

6.2. Contributions to research

This study makes three main contributions to the research on information behaviour. First, this study focuses on individuals' inward EFC and its strategies. It contributes two aspects to the knowledge of EFC in the extant ISec literature. First, although Rogers did not include EFC in the earliest PMT, he acknowledged its importance and expanded the theoretical framework in subsequent studies (Rogers, Prentice-Dunn, and Gochman 1997; Floyd, Prentice-Dunn, and Rogers 2000; Milne, Sheeran, and Orbell 2000). However, most PMT-based security behavioural research has focused on investigating users' PFC (e.g. information protecting intention), while ignoring the EFC response. Moreover, previous studies that recommended applying the full monology of PMT did not include EFC (Boss et al. 2015). We returned EFC to the PMT framework and emphasised that two coping mechanisms, PFC and EFC, should be combined to understand users' ISec behaviour. Second, inward EFC has been shown to significantly impede PFC (Chenoweth, Minch, and Gattiker 2009; Liang et al. 2019), but there is a severe lack of knowledge about inward EFC strategies in the ISec field. Although Liang et al. (2019) made a big step forward by classifying EFC, they acknowledged only three representative inward EFC strategies as components of inward EFC, and they did not investigate each strategy. In addition, the concepts on which some inward EFC strategies have been based seem to be unclear or confusing in the ISec literature. In this study, we categorised human coping systems at the theoretical level in response to the above lacunae. We also conceptualised and operationalised five highly representative inward EFC strategies, and we clarified points that seemed confusing. Moreover, we assessed and compared the roles of these strategies in PMT at the empirical level. The findings of this study could contribute to a deeper understanding of both the general concept of inward EFC and the characteristics of specific inward EFC strategies, as well as provide the foundation for developing reliable EFC theories.

The second contribution of our study is based on its theoretical discussion and empirical support. Inward EFC strategies were divided into active and passive forms. Users who adopt an active inward EFC strategy ignore or distort their perception of ISec threats; users who adopt a passive inward EFC strategy have a negative attitude towards the status quo and believe that threats are inevitable or countermeasures are useless. This classification was based not only on the interpretation of the definitions of five inward EFC strategies but also on empirical evidence of the differences in the cognitive factors that affect the two forms of inward EFC strategies. The inward EFC strategies classification clarified the differences between these strategies, thus contributing to the relevant literature and advancing the EFC-related ISec research field.

Regarding the third contribution, some findings in this study did not support some hypotheses (e.g. H3a, H4b) regarding the complexity of individual users' ISec behaviours. For example, we found a negative relationship between threat appraisal and some inward EFC strategies, which differed from most previous studies (Chen and Zahedi 2016; Liang et al. 2019). This finding indicated that contextual factors greatly affect how the individual copes (Folkman et al. 1986; Lazarus 1993). In addition, we offered a reasonable explanation for this result and suggested that minimising threats may trigger EFC adoptions in some situations. Based on these findings, we recommend that the relationship between individuals' ISec threat perceptions and inward EFC responses should be reconsidered in future research on this topic. The order of influence between threat appraisal and inward EFC strategies should also be clarified. Although the hypothesis H3 was not fully supported, the interesting and even unexpected results of the present study should lead ISec researchers to further study individual users' coping processes, thus enriching the understanding of ISec behaviour.

6.3. Implications for practice

The inward EFC of individual users to mobile malware threats not only threatens their own ISec but may also threaten the information systems of the surrounding environment (e.g. organisations, schools, and homes). However, to date, the ISec literature has studied only the influence of few EFC strategies and their cognitive processes. Such a gap in knowledge may lead to a lack of guidelines for practitioners in conducting information behaviour education and EFC training for employees. For example, if the practitioners' understanding of EFC to ISec is narrow, they may ignore some factors (e.g. perceived threat vulnerability). Perhaps prior research has shown that these factors do not significantly affect avoidance, but they could affect other EFC strategies that have gone unstudied previously. Our research explored and compared five different inward EFC strategies from theoretical and empirical perspectives and found that overlooked cognitive factors may affect EFC. This finding may increase practitioners' understanding of how to reduce EFC.

Specifically, we found that individual users' underestimation of mobile malware threats may prompt them to adopt specific EFC strategies. Various ISec reports show that attacks on smartphones and other mobile devices are increasing year by year; meanwhile, mobile malware variants have doubled (Security and Report 2018; Check Point Research 2019). Some forms of Android malware have even been developed using advanced evasion techniques to go undetected on infected devices (e.g. Triada, Lotoor). However, individual users' lack of correct awareness of mobile malware threats will lead to unrealistic optimism or overconfidence, which is not conducive to ISec actions. Therefore, organisations and public ISec educators should help users objectively recognise mobile malware threats in order to avoid inappropriate responses due to their underestimation of threats. In addition to denying or avoiding mobile malware threats, the tendency of individual users to think that mobile malware threats cannot be avoided (i.e. fatalism) also interferes with their adaptive information behaviour intent (PFC). Organisations and public information behaviour education should pay particular attention to these two kinds of EFC strategies. The findings of this study also provide insights for reducing the willingness of mobile phone users to adopt avoidance and fatalism. For example, making users aware of the seriousness of the possible consequences of mobile malware threats can make them visualise the threat instead of avoiding it. An effective way to reduce the fatalism of users is to provide effective countermeasures against mobile malware and, more importantly, convince them that the proposed countermeasures can indeed help them avoid threats adaptively. Before imparting advice on the mobile ISec behaviours of users, practitioners should ensure that these pieces of advice are feasible and easy to implement. When editing communication information for mobile phone ISec, organisations and public ISec educators can also enable users to realise the seriousness of the consequences of mobile malware without overemphasising them. This delicate balance can assure that users do not think that 'threat consequences are unavoidable.' Organisations and public ISec educators can refer to the above recommendations when training employees regarding mobile phone information security.

6.4. Limitations

This study has some limitations, including the sample (university teachers, staff, and students). The sample here cannot be generalised to other smartphone users with different backgrounds, such as different countries. That being said, the sample selection for this study is appropriate because the research focused on understanding individual users' EFC with mobile malware threats rather than the universality of EFC mechanisms. Furthermore, as Niederman and DeSanctis (1995) pointed out, research findings with students as the main research sample can often be generalised to a larger population. Student samples have been widely used in the ISec literature (Crossler and Bélanger 2014; D'Arcy, Herath, and Shoss 2014; Boss et al. 2015). As another limitation, most subjects were between the ages of 19 and 33, which is a limited age spectrum. The sample's age was also found to impact the mobile information protection intentions of individuals in this study. Thus, more research is needed on diverse demographic samples, including a larger age spectrum.

7. Conclusions

Explaining the ISec behaviour (or intention thereof) of employees is a mainstream topic in ISec research. EFC response with security threats is a recognised element influencing individuals' insecure acts. Despite the fact that ISec researchers have called for further studies on EFC, currently, only a few EFC strategies have been empirically examined in the ISec literature. Furthermore, the concept of EFC is sometimes convoluted in the ISec literature. As a result, ISec scholars and practitioners reading ISec papers on EFC may (1) have a limited conception of EFC or (2) confuse it with other concepts. In this study, we differentiated five inward

EFC strategies and tested them empirically in the context of mobile malware. The key results indicate that response efficacy has the greatest beneficial effect because it reduces the willingness of individual users to adopt reactance, fatalism, wishful thinking, and hopelessness coping strategies. Individual users' vulnerability perception of the threat likewise positively affects their willingness to adopt passive EFC strategies. Among the five inward EFC strategies, avoidance and fatalism significantly weaken the intention of individual users to protect their mobile phone ISec (PFC).

Notes

1. Based on Proofpoint's 2020 user risk report (User risk report 2020), 45% of users admitted to password reuse; more than 50% did not password-protect home Wi-Fi networks; 90% of working adults admitted to using employer-issued devices for personal activities; nearly 50% allowed friends and family to access their work devices (p.4).
2. Note that both EFC and EFC strategies refer to personal responses to regulate stressful emotions (Folkman and Lazarus 1980). Although it is called the EFC strategy, because its nature is the same as that of EFC, it is classified as EFC (Skinner et al. 2003). See Section 2 for further details.
3. Folkman and Lazarus (1980) referred to coping processes as 'what the person actually thinks and does in a particular encounter and to changes in these efforts as the encounter unfolds during a single episode or across episodes that are in some sense part of a common stressful encounter' (p. 224).
4. According to Milne, Sheeran, and Orbell (2000), protection motivation is synonymous with the intention to perform a behavior.
5. Lazarus and Launier (1978) proposed that a stressor (or an event) can be construed as a loss, a threat, or a challenge. Threat refers to damage that is anticipated and may or may not be inevitable. In this paper, mobile malware threat is defined as anticipated damage related to IS caused by mobile malware, which may or may not be inevitable.

Disclosure statement

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

References

2020 Cyber Threats. 2020. https://www.netwrix.com/2020_cyber_threats_report.html.

Abraham, C. S., P. Sheeran, D. Abrams, and R. Spears. 1994. "Exploring Teenagers' Adaptive and Maladaptive Thinking in Relation to the Threat of HIV Infection." *Psychology and Health* 9 (4): 253–272.

Bagozzi, R. P., Y. Yi, and L. W. Phillips. 1991. "Assessing Construct Validity in Organizational Research." *Administrative Science Quarterly* 36 (3): 421–458.

Bandura, A. 1999. "Moral Disengagement in the Perpetration of Inhumanities." *Personality and Social Psychology Review* 3 (3): 193–209.

Bandura, A. 2002. "Selective Moral Disengagement in the Exercise of Moral Agency." *Journal of Moral Education* 31 (2): 101–119.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. 2015. "What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors." *MIS Quarterly* 39 (4): 837–864.

Brehm, J. W. 1966. *A theory of psychological reactance*.

Brehm, S. S., and J. W. Brehm. 1981. *Psychological Reactance: A Theory of Freedom and Control*. New York: Academic Press.

Burgoon, M., E. Alvaro, J. Grandpre, and M. Voulodakis. 2002. *The Persuasion Handbook: Developments in Theory and Practise*, 213–232. Thousand Oaks, CA: Sage Publications.

Carver, C. S., M. F. Scheier, and J. K. Weintraub. 1989. "Assessing Coping Strategies: A Theoretically Based Approach." *Journal of Personality and Social Psychology* 56 (2): 267.

Check Point Research. 2019. *Cyber Attack Trends: 2019 Mid-Year Report*. https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/.

Chen, Y., and F. M. Zahedi. 2016. "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China." *MIS Quarterly* 40 (1): 205–222.

Chenoweth, T., R. Minch, and T. Gattiker. 2009. "Application of Protection Motivation Theory to Adoption of Protective Technologies." System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference On, 1–10.

Cramer, P. 2000. "Defense Mechanisms in Psychology Today: Further Processes for Adaptation." *American Psychologist* 55 (6): 637.

Crossler, R., and F. Bélanger. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument." *ACM Sigmis Database* 45 (4): 51–71.

Dang-Pham, D., and S. Pittayachawan. 2015. "Comparing Intention to Avoid Malware Across Contexts in a BYOD-Enabled Australian University: A Protection Motivation Theory Approach." *Computers & Security* 48: 281–297.

D'Arcy, J., T. Herath, and M. K. Shoss. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective." *Journal of Management Information Systems* 31 (2): 285–318.

Del Greco, L., W. Walop, and L. Eastridge. 1987. "Questionnaire Development: 3. Translation." *CMAJ: Canadian Medical Association Journal* 136 (8): 817.

Dillman, D. A., J. D. Smyth, and L. M. Christian. 2014. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. Hoboken, NJ: John Wiley & Sons.

Eppright, D. R., J. B. Hunt, J. F. Tanner Jr, and G. R. Franke. 2003. "Fear, Coping, and Information: A Pilot Study on Motivating a Healthy Response." *Health Marketing Quarterly* 20 (1): 51–73.

Felt, A. P., M. Finifter, E. Chin, S. Hanna, and D. Wagner. 2011. "A Survey of Mobile Malware in the Wild."

Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile devices, 3–14.

Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. 2000. "A Meta-Analysis of Research on Protection Motivation Theory." *Journal of Applied Social Psychology* 30 (2): 407–429.

Folkman, S., and R. S. Lazarus. 1980. "An Analysis of Coping in a Middle-Aged Community Sample." *Journal of Health and Social Behavior* 21 (3): 219–239.

Folkman, S., and R. S. Lazarus. 1985. "If it Changes it Must be a Process: Study of Emotion and Coping During Three Stages of a College Examination." *Journal of Personality and Social Psychology* 48 (1): 150.

Folkman, S., R. S. Lazarus, R. J. Gruen, and A. DeLongis. 1986. "Appraisal, Coping, Health Status, and Psychological Symptoms." *Journal of Personality and Social Psychology* 50 (3): 571.

Fornell, C., and D. F. Larcker. 1981. *Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics*. Los Angeles, CA: Sage Publications Sage CA.

Fruin, D. J., C. Pratt, and N. Owen. 1992. "Protection Motivation Theory and Adolescents' Perceptions of Exercise." *Journal of Applied Social Psychology* 22 (1): 55–69.

Fry, R. B., and S. Prentice-Dunn. 2005a. "Effects of a Psychosocial Intervention on Breast Self-Examination Attitudes and Behaviors." *Health Education Research* 21 (2): 287–295.

Fry, R. B., and S. Prentice-Dunn. 2005b. "Effects of Coping Information and Value Affirmation on Responses to a Perceived Health Threat." *Health Communication* 17 (2): 133–147.

Gardner, M., and L. Steinberg. 2005. "Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: an Experimental Study." *Developmental Psychology* 41 (4): 625.

Gefen, D., and D. Straub. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example." *Communications of the Association for Information Systems* 16 (1): 5.

Gefen, D., D. Straub, and M.-C. Boudreau. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice." *Communications of the Association for Information Systems* 4 (1): 7.

Hair, J. F., R. E. Anderson, R. L. Tatham, and C. William. 1998. *Black (1998), Multivariate Data Analysis*. Upper Saddle River, NJ: Prentice Hall.

Herath, T., and H. R. Rao. 2009. "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18 (2): 106–125. doi:10.1057/ejis.2009.6.

Hox, J. J., and C. J. M. Maas. 2001. "The Accuracy of Multilevel Structural Equation Modeling with Pseudobalanced Groups and Small Samples." *Structural Equation Modeling* 8 (2): 157–174.

IBM. 2019. Cost of a data breach report. In *IBM Security*. https://www.ibm.com/downloads/cas/ZBZLY7KL.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95.

Johnston, A. C., and M. Warkentin. 2010. "Fear Appeals and Information Security Behaviors: an Empirical Study." *MIS Quarterly* 34 (3): 549–566.

Johnston, A. C., M. Warkentin, and M. T. Siponen. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric." *MIS Quarterly* 39 (1): 113–134.

Jung, J.-H., D. H. Kim, Y. Sung, and J. Lee. 2016. "Exploring the Relationship Between Psychological Distance and Motivations to use Media." 2016 global Marketing Conference at Hong Kong, 1130.

Kazak, A. E., and A. T. Meadows. 1989. "Families of young adolescents who have survived cancer: Social-emotional adjustment, adaptability, and social support." Journal of Pediatric Psychology 14 (2): 175–191.

Kline, R. B. 2011. *Principles and Practice of Structural Equation Modeling 3rd ed.* New York, NY: The Guilford Press.

Lazarus, R. S. 1966. *Psychological stress and the coping process*.

Lazarus, R. S. 1993. "Coping Theory and Research: Past, Present, and Future." Psychosomatic Medicine 55: 234–247.

Lazarus, R. S., and S. Folkman. 1984. *Stress, Appraisal, and Coping*. New York: Springer Publishing Company.

Lazarus, R. S., and R. Launier. 1978. "Stress-related Transactions Between Person and Environment." In *Perspectives in Interactional Psychology*, 287–327. Boston, MA: Springer.

Liang, H., and Y. Xue. 2009. "Avoidance of Information Technology Threats: a Theoretical Perspective." *MIS Quarterly* 33 (1): 71–90.

Liang, H., and Y. Xue. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *Journal of the Association for Information Systems* 11 (7): 394.

Liang, H., Y. Xue, A. Pinsonneault, and Y. Wu. 2019. "What Users do Besides Problem-Focused Coping When Facing it Security Threats: An Emotion-Focused Coping Perspective." *MIS Quarterly* 43 (2): 373–394.

Livneh, H. 2000. "Psychosocial Adaptation to Cancer: The Role of Coping Strategies." *Journal of Rehabilitation* 66 (2): 40–49.

Lowry, P. B., and G. D. Moody. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies." *Information Systems Journal* 25 (5): 433–463.

McCrae, Robert R. 1984. "Situational Determinants of Coping Responses: Loss, Threat, and Challenge." *Journal of Personality and Social Psychology* 46 (4): 919.

McCrae, R. R., and P. T. Costa. 1986. "Personality, Coping, and Coping Effectiveness in an Adult Sample." *Journal of Personality* 54 (2): 385–404.

McMath, B. F., and S. Prentice-Dunn. 2005. "Protection Motivation Theory and Skin Cancer Risk: The Role of Individual Differences in Responses to Persuasive Appeals." *Journal of Applied Social Psychology* 35 (3): 621–643.

Meade, A. W., and S. B. Craig. 2012. "Identifying Careless Responses in Survey Data." *Psychological Methods* 17 (3): 437.

Milne, S., S. Orbell, and P. Sheeran. 2002. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and

Implementation Intentions." *British Journal of Health Psychology* 7 (2): 163–184.

Milne, Sarah, P. Sheeran, and S. Orbell. 2000. "Prediction and Intervention in Health-related Behavior: A Meta-analytic Review of Protection Motivation Theory." *Journal of Applied Social Psychology* 30 (1): 106–143.

Moody, G. D., M. Siponen, and S. Pahnila. 2018. "Toward a Unified Model of Information Security Policy Compliance." *MIS Quarterly* 42 (1): 285–311.

Mwagwabi, F., T. McGill, and M. Dixon. 2014. "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines." System Sciences (HICSS), 2014 47th Hawaii International Conference On, 3188–3197.

Ng, B.-Y., A. Kankanhalli, and Y. C. Xu. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective." *Decision Support Systems* 46 (4): 815–825.

Niederman, F., and G. DeSanctis. 1995. "The Impact of a Structured-Argument Approach on Group Problem Formulation." *Decision Sciences* 26 (4): 451–474.

Nunnally, J. C., I. H. Bernstein, and J. M. T. Berge. 1978. *Psychometric Theory (Vol. 3)*. New York: McGraw-Hill.

Pearlin, L. I., and C. Schooler. 1978. "The Structure of Coping." *Journal of Health and Social Behavior* 19 (1): 2–21.

Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology* 88 (5): 879.

Prentice-Dunn, S., D. L. Floyd, and J. M. Flournoy. 2001. "Effects of Persuasive Message Order on Coping with Breast Cancer Information." *Health Education Research* 16 (1): 81–84.

Rippetoe, P. A., and R. W. Rogers. 1987. "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat." *Journal of Personality and Social Psychology* 52 (3): 596.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude change1." *The Journal of Psychology* 91 (1): 93–114.

Rogers, R. W. 1983. *Social Psychophysiology: A Sourcebook*, 153–176. New York: Guilford Press.

Rogers, R. W., S. Prentice-Dunn, and D. S. Gochman. 1997. *Handbook of Health Behavior Research 1: Personal and Social Determinants*. New York, NY, US: Plenum Press.

Ruiter, R. A. C., C. Abraham, and G. Kok. 2001. "Scary Warnings and Rational Precautions: A Review of the Psychology of Fear Appeals." *Psychology and Health* 16 (6): 613–630.

Security, I., and T. Report. 2018. *Internet Security Threat Report 23 Volume*. https://docs.broadcom.com/doc/istr-23-executive-summary-en.

Seiffge-Krenke, I. 2004. "Adaptive and Maladaptive Coping Styles: Does Intervention Change Anything?" *European Journal of Developmental Psychology* 1 (4): 367–382.

Self, C. A., and R. W. Rogers. 1990. "Coping with Threats to Health: Effects of Persuasive Appeals on Depressed, Normal, and Antisocial Personalities." *Journal of Behavioral Medicine* 13 (4): 343–357.

Siponen, M. T. 2000. "Conceptual Foundation for Organizational Information Security Awareness." *Information Management and Computer Security* 8 (1): 31–41. doi:10.1108/09685220010371394.

Skinner, E. A., K. Edge, J. Altman, and H. Sherwood. 2003. "Searching for the Structure of Coping: a Review and Critique of Category Systems for Classifying Ways of Coping." *Psychological Bulletin* 129 (2): 216.

Straub, D., M.-C. Boudreau, and D. Gefen. 2004. "Validation Guidelines for IS Positivist Research." *Communications of the Association for Information Systems* 13 (1): 24.

Tehseen, S., T. Ramayah, and S. Sajilan. 2017. "Testing and Controlling for Common Method Variance: A Review of Available Methods." *Journal of Management Sciences* 4 (2): 142–168.

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

Tsai, H. S., M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten. 2016. "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective." *Computers & Security* 59: 138–150.

Umeh, K. 2004. "Cognitive Appraisals, Maladaptive Coping, and Past Behaviour in Protection Motivation." *Psychology & Health* 19 (6): 719–735.

User Risk Report. 2020. In *Proofpont* (Vol. 234). https://www.proofpoint.com/au/resources/white-papers/user-risk-report.

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49 (3): 190–198.

Van der Velde, F. W., and J. Van der Pligt. 1991. "AIDS-related Health Behavior: Coping, Protection Motivation, and Previous Behavior." *Journal of Behavioral Medicine* 14 (5): 429–451.

Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis. 2003. "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* 27 (3): 425–478.

Weinstein, N. D. 1980. "Unrealistic Optimism About Future Life Events." *Journal of Personality and Social Psychology* 39 (5): 806.

Weinstein, N. D. 1982. "Unrealistic Optimism About Susceptibility to Health Problems." *Journal of Behavioral Medicine* 5 (4): 441–460.

Witte, K. 1991. "The Role of Threat and Efficacy in AIDS Prevention." *International Quarterly of Community Health Education* 12 (3): 225–249.

Witte, K. 1992. "Putting the Fear Back Into Fear Appeals: The Extended Parallel Process Model." *Communications Monographs* 59 (4): 329–349.

Witte, K. 1994. "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM)." *Communications Monographs* 61 (2): 113–134.

Witte, K. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale." *Journal of Health Communication* 1 (4): 317–342.

Witte, K., and M. Allen. 2000. "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns." *Health Education & Behavior* 27 (5): 591–615.

Woon, I., G.-W. Tan, and R. Low. 2005. "A Protection Motivation Theory Approach to Home Wireless Security." ICIS 2005 proceedings, 31.

Zahedi, F. M., A. Abbasi, and Y. Chen. 2015. "'Individuals' use and Enhance Their Performance." *Journal of the Association for Information Systems* 16 (6): 448.

Appendices

Appendix A. Participants profile

Profile variables	Mean		SD	
Age	21.87		4.60	
Information importance stored in the mobile	6.05		0.06	
Previous exposure to similar ISec threats	3.17		0.09	
Gender	**Male**		**Female**	
	276 (67.73%)		132 (32.27%)	
Profession	**Student**		**Staff**	
	361(88.92%)		45(11.08%)	
Mobile operating system (OS)	**Android**	**iOS**		**other**
	318 (77.94%)	88 (21.57%)		2 (0.49%)
Experience of using mobile phone	**≤ 1 year**	**1 year - 2 years**	**2 years - 4 years**	**≥ 4 years**
	35 (8.58%)	82 (20.10%)	127 (31.13%)	164 (40.20%)

As shown in the table above, we investigated seven profile variables related to participants and their mobile phones. These seven variables are also the control variables of this paper. Among them, two variables are latent variables: Previous exposure to similar ISec threats, Information importance stored in the mobile. They were measured with 3 items respectively (see Appendix B.1). The reliability and validity of these two variables are reported in Appendix B.3 and B.4.

Participants ranged in age from 18 to 46, 90% of them were under 28 years old. Most of participants are students. Male participants are twice as many as female participants. Most of the participants use Android phones and have more than two years of experience with mobile phones. According to the average, participants have important information stored in their mobile phones, and have been less exposed to similar ISec threats in their previous experience.

It is worth mentioning that the proportions of gender, occupation, and mobile OS in this research sample are unevenly distributed. It is often the case with random sampling, but it will not significantly interfere with the study results. We use structural equation modeling analysis and ANOVA analysis in this study. Based on the assumptions of structural equation modeling and ANOVA (Kline 2011), the unequal sample sizes may affect the heterogeneity of variance in ANOVA analysis. However, the STATA statistical software we use can automatically handle unequal samples through weighted average, Dunnett's test, and other methods (https://www.stata.com/stata-news/news28-4/power-and-sample-size/), which can decrease the type I error and increase the statistical power. For structural equation modeling, it is not a problem because this is a within-group analysis, and the sample size is large enough (Hox and Maas 2001).

Appendix B. Supplement to research methods and data analysis

B.1. Survey instrument

Constructs	Item name	Item	Resource
Threat severity	Sev1	If my mobile phone is infected with malware, it would be severe.	*Adapted from* Witte (1996), Milne, Orbell, and Sheeran (2002)
	Sev2	If my mobile phone is infected with malware, it would be significant.	
	Sev3	If my mobile phone is invaded by malware, I would suffer a lot of pain.	
Threat vulnerability	Vul1	My mobile phone is at risk for becoming infected by malware.	*Adapted from* Witte (1996)
	Vul2	It is likely that my mobile phone will become infected by malicious applications.	
	Vul3	It is possible that my mobile phone will become infected by malicious programmes.	
Response efficacy	Res1	Updating mobile operating system is effective for preventing my phone from being infected with malware.	*Adapted from* Witte (1996), Milne, Orbell, and Sheeran (2002)
	Res2	When updating mobile operating system timely, a mobile phone is more likely to be protected.	
	Res3	If I were to update mobile operating system timely, the chances of my phone being infected with malware will be lessened.	
Self-efficacy	Sel1	Updating mobile operating system timely would be easy for me.	*Adapted from* Witte (1996), Milne, Orbell, and Sheeran (2002)
	Sel2	It would not be difficult for me to update the mobile operating system timely.	
	Sel3		

(*Continued*)

Continued.

Constructs	Item name	Item	Resource
		I am able to update the mobile operating system timely without much effort.	
PFC intention	Int1	I intend to update my mobile operating system timely in the future.	*Adapted from* Venkatesh et al. (2003)
	Int2	I predict I will update my mobile operating system timely in the future.	
	Int3	I plan to update my mobile operating system timely in the future.	
Avoidance	Avoid1	I try not to think about the possibility of my mobile phone being infected by mobile malware.	*Adapted from* Rippetoe and Rogers (1987)
	Avoid2	I try not to think about the serious consequences of my mobile phone being infected by mobile malware.	
	Avoid3	I try not to think that my mobile phone is very likely to be infected by mobile malware.	
Reactance	React1	To what degree do you: Feel that problems of mobile malware are overly exaggerated?	*Adapted from* Witte (1992, 1996)
	React2	To what degree do you: Think that problems of mobile malware are overstated?	
Hopelessness	Hope1	Given what I know about mobile malware, I sometimes feel updating mobile operating system is almost useless to protect my mobile phone.	*Adapted from* Rippetoe and Rogers (1987)
	Hope2	I believe that updating the mobile operating system has no effect on preventing mobile malware infection.	
	Hope3	Regularly updating the mobile operating system does not help to prevent mobile malware infection.	

(*Continued*)

Continued.

Constructs	Item name	Item	Resource
Fatalism	Fata1	Using anti-malware software isn't going to help; if my mobile phone is going to be infected by malware, it will be infected anyway.	*Adapted from* Rippetoe and Rogers (1987), Eppright et al. (2003)
	Fata2	Only time will tell if my mobile phone gets a malware; nothing can be done about it.	
	Fata3	If my mobile phone is destined to get a malware, it will; there is little I can do about it.	
Wishful thinking	Wish1	I believe my mobile phone is self-protecting and does not require me to do anything.	*Adapted from* Rippetoe and Rogers (1987)
	Wish2	I believe that one day mobile malware will be completely wiped out.	
	Wish3	I believe there will always be someone to help me when my mobile phone receives a malware threat.	
Important information on the mobile	Assim1	Some files stored on my mobile phone are important to me.	
	Assim2	Some data stored on my mobile phone are critical to me.	
	Assim3	Some critical information is stored on my mobile phone.	
Previous exposure to similar ISec threat	Otherex1	I have suffered from a similar information security threat in the past. (Liang and Xue 2010)	*Adapted from* Liang and Xue (2010), Zahedi, Abbasi, and Chen (2015)
	Otherex2	I have ever had a similar information security threat when using a mobile phone in the past. (Chai et al. 2009)	
	Otherex3	The number of similar threat I have encountered in the past has been (very low/very high). (Zahedi, Abbasi, and Chen 2015).	

Note*:* all items in our measurement instrument were evaluated on a 7-point Likert scale.

B.2. Validation of instrument's content validity.

To ensure content validity, we performed both the pre-test, questionnaire translation procedure and pilot test in addition to the literature review. In the pre-test, we established an expert panel of seven teachers and doctoral students from the faculty of information and technology (IT) who are proficient in quantitative research methods. The expert panel gave constructive comments on several aspects, such as whether the adapted items in the questionnaire reflected the constructs that to be tested, whether the questionnaire meets to the research purpose and context, the rigour of the wording and so on. After the content validity panel review, one item of threat severity and one item of threat vulnerability are deleted because of redundant, and some vocabulary and grammar were corrected. Since the sample is from China, the questionnaire was translated to accommodate Chinese participants. We implemented the questionnaire translation procedure according to the steps recommended by Del Greco, Walop, and Eastridge (1987). Specifically, 1) the questionnaire was preliminarily translated into Chinese by a bilingual subject in the IT faculty, 2) each translated item of the preliminary translation was compared by another bilingual subject according to their content, meaning, and expression clarity, 3) cross-language equivalence was tested by executing both the translated and original forms of the questionnaire to 3 new bilingual subjects after the results of the second step were acceptable. The results show that the translated questionnaire reflects the original questionnaire well. To make sure if the participants understood the items in the expected manner, a small pilot study was conducted with a subsample of the population (30 sample sizes) to evaluate the questionnaire. The purpose of the pilot study is to determine whether the proposed questionnaire and procedures are suitable for the larger study, which constitutes a final test of the exact questionnaire and implementation procedures used in the study. It provides valuable information on 1) how the various items and the overall structure of the questionnaire works, 2) how research procedures will work in practice (Dillman, Smyth, and Christian 2014). The results of the pilot test showed that the small sample understood the overall questionnaire and each item.

B.3. Standardised confirmatory factor loadings including latent control variables.

Constructs	Items	Loading	z-value	p-value
Threat severity	Sev1	0.779	28.27	0.000
	Sev2	0.795	28.88	0.000
	Sev3	0.754	25.77	0.000
Threat vulnerability	Vul1	0.924	60.28	0.000
	Vul2	0.809	38.36	0.000
	Vul3	0.825	41.43	0.000
Response efficacy	Res1	0.866	50.34	0.000
	Res2	0.889	56.97	0.000
	Res3	0.826	42.46	0.000
Self-efficacy	Sel1	0.932	73.80	0.000
	Sel2	0.804	40.12	0.000
	Sel3	0.895	62.28	0.000
PFC intention	Int1	0.819	46.27	0.000
	Int2	0.924	90.59	0.000
	Int3	0.969	118.66	0.000
Avoidance	Avoid1	0.899	57.63	0.000
	Avoid2	0.886	54.70	0.000
	Avoid3	0.808	39.11	0.000
Reactance	React1	0.886	34.87	0.000
	React2	0.955	37.79	0.000
Hopelessness	Hope1	0.855	58.54	0.000
	Hope2	0.950	111.00	0.000
	Hope3	0.923	92.99	0.000
Fatalism	Fata1	0.817	40.16	0.000
	Fata2	0.835	41.77	0.000
	Fata3	0.906	55.82	0.000
Wishful thinking	Wish1	0.825	33.99	0.000
	Wish2	0.821	33.83	0.000
	Wish3	0.750	26.92	0.000
Important information on the mobile	Assim1	0.914	80.81	0.000
	Assim2	0.888	68.40	0.000
	Assim3	0.929	89.11	0.000
Previous exposure to similar ISec threats	Otherex1	0.926	110.76	0.000
	Otherex2	0.933	119.42	0.000
	Otherex3	0.980	190.95	0.000

(Continued)

Continued.

B.4. Exploratory factor loadings including latent control variables.

Constructs	Items	Loading	AVE	CR	Cronbach Alpha
Threat severity	Sev1	0.769	0.562	0.794	0.820
	Sev2	0.719			
	Sev3	0.690			
Threat vulnerability	Vul1	0.873	0.597	0.813	0.838
	Vul2	0.784			
	Vul3	0.814			
Response efficacy	Res1	0.766	0.673	0.860	0.892
	Res2	0.861			
	Res3	0.802			
Self-efficacy	Sel1	0.896	0.731	0.890	0.906
	Sel2	0.797			
	Sel3	0.876			
PFC intention	Int1	0.766	0.757	0.903	0.918
	Int2	0.939			
	Int3	0.928			
Avoidance	Avoid1	0.855	0.720	0.885	0.898
	Avoid2	0.862			
	Avoid3	0.804			
Reactance	React1	0.888	0.781	0.877	0.911
	React2	0.892			
Hopelessness	Hope1	0.787	0.794	0.920	0.939
	Hope2	0.931			
	Hope3	0.892			
Fatalism	Fata1	0.825	0.685	0.867	0.888
	Fata2	0.723			
	Fata3	0.885			
Wishful thinking	Wish1	0.729	0.123	0.218	0.490
	Wish2	0.811			
	Wish3	0.691			
Important information on the mobile	Assim1	0.883	0.882	0.957	0.929
	Assim2	0.869			
	Assim3	0.913			
Previous exposure to Similar ISec threats	Otherex1	0.930	0.790	0.919	0.962
	Otherex2	0.932			
	Otherex3	0.956			

Appendix C. Discussion and verification of the core structure of PMT

Due to space limitations, the results of the PMT core structure will be discussed and analyzed here.

As reported in Table 7 of the main text, response efficiency (β=0.463, p=0.000) and self-efficacy (β=0.273, p=0.000) have significant positive impacts on individual users' PFC intention, but not threat severity (β=−0.085, p≥0.05) and vulnerability (β=0.102, p≥0.05). The relationship between the original factors of the PMT research model is generally consistent with most of the previous studies. The individual users' response efficacy and self-efficacy increase their PFC intentions. However, threat severity and threat vulnerability are not clearly linked to the individual user's PFC intention. Although this result violated the general assumptions of PMT, Milne, Sheeran, and Orbell (2000)'s meta-analysis of PMT found that the association between threat appraisal and protection behavioral intention is small. Some previous ISec studies also had consistent results (Ng, Kankanhalli, and Xu 2009; Mwagwabi, McGill, and Dixon 2014; Dang-Pham and Pittayachawan 2015; Tsai et al. 2016), it may either because the result is affected by the extraneous factors (Ifinedo 2012), or because there are other factors (e.g. attitude, concern level) that act as moderators between threat appraisal and protection intention (Herath and Rao 2009).

Appendix D. The role of control variables

As mentioned in Appendix B, the seven control variables in this study are: age, gender, profession, mobile malware operating system, previous experience of using mobile phone, information importance stored in the mobile phone, previous exposure to the similar ISec threat. After analyzing the research model, some interesting findings of the effect of three control variables (i.e. age, operating system, information importance stored in the mobile phone) on individual users' mobile phone PFC intention were found.

1) The age of the participants (β=0.037, p=0.015) has a significant positive impact on their protection motivation. It means that as the age increases, the intention of individual users to timely update their mobile OS is enhanced. It is understandable since younger people are proving to be more prone to risk behaviour and risky decision making (Gardner and Steinberg 2005), which may lead to the lower level of protection intent when they are in the face of information related risk.
2) Individual users who using the iOS operating system have obviously lower protection motivation than who using other mobile operating systems (β=−0.36, p=0.029). Main reasons behind this finding may be that Apple is successful in identifying and blocking malware, and malware authors are not targeting iOS users because of the SMS restrictions (Felt et al. 2011). As a result, iOS users are less exposed to mobile malware threats and more likely to relax their vigilance, thus they have relatively weak PFC intentions.

Appendix E. The impact of participants' different backgrounds on their preference for inward EFC strategies

This study's control variables cover the subjects' primary background information (gender, age, occupation, mobile OS, previous experience using mobile phones, importance of the information stored on the mobile phone, previous exposure to a similar ISec threat). We conducted a series of ANOVA and regression analyses to investigate the influence of participants' different backgrounds on inward EFC strategies adoption. The following tables show the results.

E.1. The impact of gender on the five inward EFC strategies

	Gender		ANOVA results	
Dependent variables	Male	Female	F value	*p*-value
Avoidance	4.12	4.00	0.63	0.43
Reactance	3.00	3.00	0.01	0.91
Hopelessness	3.02	3.03	0.01	0.93
Wishful thinking	2.72	2.78	0.24	0.62
Fatalism	3.37	3.07	3.13	0.08

E.2. The impact of profession on the five inward EFC strategies

	Profession		ANOVA results	
Dependent variables	Student	Staff	F value	*p*-value
Avoidance	4.10	4.00	0.16	0.69
Reactance	3.00	3.01	0.00	0.99
Hopelessness	2.96	3.53	6.77	0.01
Wishful thinking	2.69	3.19	7.14	0.01
Fatalism	3.23	3.62	2.32	0.13

E.3. The impact of age on the five inward EFC strategies

	Age			ANOVA results	
Dependent variables	18–24	25–34	35–46	F value	*p*-value
Avoidance	4.10	4.04	3.89	0.12	0.89
Reactance	3.01	2.79	3.63	1.72	0.18
Hopelessness	2.96	3.35	4.00	4.35	0.01
Wishful thinking	2.69	3.23	3.06	3.66	0.03
Fatalism	3.23	3.67	3.50	1.20	0.30

E.4. The impact of mobile OS on the five inward EFC strategies

	Operation System			ANOVA results	
Dependent variables	Android	iOS	Other	F value	*p*-value
Avoidance	4.08	4.12	3.33	0.26	0.77
Reactance	2.98	3.07	4.50	1.39	0.25
Hopelessness	2.95	3.29	2.00	2.56	0.08
Wishful thinking	2.66	3.03	3.00	3.43	0.03
Fatalism	3.27	3.31	1.67	1.00	0.37

E.5. The impact of previous using experience on the five inward EFC strategies

	Previous experience using mobile phones				ANOVA results	
Dependent variables	<1 year	1–2 years	2–4 years	>4 years	F value	*p*-value
Avoidance	4.55	3.89	4.10	4.08	1.48	0.22
Reactance	3.09	3.06	3.04	2.94	0.24	0.87

(*Continued*)

Continued.

Dependent variables	Previous experience using mobile phones				ANOVA results	
	<1 year	1–2 years	2–4 years	>4 years	F value	*p*-value
Hopelessness	3.32	3.01	2.94	3.02	0.68	0.57
Wishful thinking	3.30	2.75	2.62	2.71	3.04	0.03
Fatalism	3.32	3.44	3.20	3.24	0.42	0.74

E.6. The impact of previous using experience on the five inward EFC strategies

	Importance of the information stored on the mobile phone (regression analysis)			
Dependent variables	Coefficient	S.E.	t value	*p*-value
Avoidance	−0.10	0.06	−1.63	0.10
Reactance	−0.24	0.06	−4.39	0.00
Hopelessness	−0.18	0.06	−3.16	0.00
Wishful thinking	−0.17	0.05	−3.50	0.00
Fatalism	−0.06	0.07	−0.80	0.42

E.7. The impact of previous using experience on the five inward EFC strategies

	Previous exposure to a similar ISec threat (regression analysis)			
Dependent variables	Coefficient	S.E.	t value	*p*-value
Avoidance	−0.08	0.04	−2.05	0.04
Reactance	−0.03	0.04	−0.85	0.40
Hopelessness	0.04	0.04	0.99	0.32
Wishful thinking	0.00	0.03	0.04	0.97
Fatalism	−0.07	0.04	1.58	0.11

Since some background information has more than two categories, we conducted Tukey's post-hoc analysis and got more detailed results. We then try to make explanations for each finding.

1) Compared with 18–24 years old, participants aged 35–46 felt more hopeless when faced with mobile malware threats ($p<0.05$); participants aged 25–34 were more willing to adopt wishful thinking ($p<0.05$). Based on previous health psychology literature, we think it may be related to their low coping appraisal (Umeh 2004; McMath and Prentice-Dunn 2005; Fry and Prentice-Dunn 2005b). Participants aged 35–46 may lack of the countermeasures or feel incompetent due to their limited knowledge of smartphones and malwares. As a result, they emotionally hope the malware threat can disappear without their effort, or even feel helplessness.
2) Participants who use iOS are more inclined to adopt wishful thinking than those who use Android ($p<0.05$). The reason is probably what we mentioned in Appendix D, that is, iOS has a stronger ability to protect users' information security than other OS such as Android because of its characteristics.
3) Participants with less than one year of mobile phone using experience showed a significant preference for wishful thinking strategy than those with more than two years of experience ($p<0.05$). It may be because users with relatively short-term experience in using smartphones lack accurate knowledge of mobile malware, thus have unrealistic illusions about how to deal with threats.

References

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication* 52(2), 167–182.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281–297.

Del Greco, L., Walop, W., & Eastridge, L. (1987). Questionnaire development: 3. Translation. *CMAJ: Canadian Medical Association Journal*, *136*(8), 817.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: the tailored design method*. John Wiley & Sons.

Eppright, D. R., Hunt, J. B., Tanner Jr, J. F., & Franke, G. R. (2003). Fear, coping, and information: A pilot study on motivating a healthy response. *Health Marketing Quarterly*, *20*(1), 51–73.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 3–14.

Fry, R. B., & Prentice-Dunn, S. (2005). Effects of coping information and value affirmation on responses to a perceived health threat. *Health Communication*, *17*(2), 133–147.

Gardner, M., & Steinberg, L. (2005). Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental Psychology*, *41*(4), 625.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18* (2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hox, J. J., & Maas, C. J. M. (2001). The accuracy of multilevel structural equation modeling with pseudobalanced groups and small samples. *Structural Equation Modeling*, *8*(2), 157–174.

Ifinedo, *P.* (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

Kline, R. B. (2011). *Principles and practice of structural equation modeling 3 rd ed*. New York, NY, The Guilford Press.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394.

McMath, B. F., & Prentice-Dunn, S. (2005). Protection motivation theory and skin cancer risk: The role of individual differences in responses to persuasive appeals. *Journal of Applied Social Psychology*, *35*(3), 621–643.

Milne, S., Orbell, S., & Sheeran, *P.* (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, *7*(2), 163–184.

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. *System Sciences (HICSS), 2014 47th Hawaii International Conference On*, 3188–3197.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150.

Umeh, K. (2004). Cognitive appraisals, maladaptive coping, and past behaviour in protection motivation. *Psychology & Health*, *19*(6), 719–735.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329–349.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–342.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448.