Computers & Security 140 (2024) 103776

Contents lists available at ScienceDirect

Computers & Security

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

Testing the dominant mediator in EPPM: An empirical study on household anti-malware software users

Yitian Xie [a,*], Mikko Siponen [b], Gabriella Laatikainen [c], Gregory D. Moody [d], Xiaosong Zheng [e]

[a] Assistant Professor, Xi'an Jiaotong-Liverpool University, China
[b] Professor of Information Systems, Information Systems, Statistics, and Management Science Culverhouse College of Business, The University of Alabama, United States
[c] Senior Scientist, VTT Technical Research Centre of Finland, Finland
[d] Department of Management Information Systems, University of Nevada, Las Vegas, United States
[e] Professor of Accounting, Shanghai University, China

ARTICLE INFO

Keywords:
The extended parallel process model (EPPM)
Dominant mediator
Contrast hypothesis
Multiple mediation analysis
Danger control process
Fear control process

ABSTRACT

A key research area in information systems security (ISec) is explaining or improving users' IS security outcomes via the extended parallel process model (EPPM) lens. While the theoretical construct in emotional valence (e.g., fear) and cognitive valence (e.g., perceived efficacy) were deemed as mediators in previous EPPM-related ISec studies, existing research has ignored the value of testing and reporting the dominant mediator between the emotional valence and the cognitive valence. In this paper, we reintroduce the theoretical origins of the *dominant mediator assumption* in EPPM and highlight its merits using the multiple mediation method. Theoretically, we illustrate how testing and reporting the dominant mediator can help identify the dominant mechanism triggering specific behavioral outcomes. Further, this paper questions the dominant mediating role of *fear* on the behavioral outcome in ISec context. Methodologically, this study proposes to assess the dominant mediator via a multiple mediation model instead of using the discriminant value equation introduced by Witte (1995), Witte et al. (1996) and enhanced by Chen et al. (2021) when testing the EPPM theory in the ISec context.

1. Introduction

A key research area in information systems security (ISec) is explaining or improving users' IS security outcomes via the extended parallel process model (EPPM) lens. Recently, behavioral ISec has started to scrutinize and debate the fundamental assumptions of EPPM (Boss et al., 2015; Chen et al., 2021; Lowry et al., 2023; Moody et al., 2018). Dominant mediation, the assumption that individuals' behavior is driven by either danger control or fear control processes, is a fundamental theoretical assumption in EPPM (Witte, 1992, 1994). As noted by Witte (1994, p. 115), "According to the EPPM, the evaluation of a fear appeal initiates two appraisals of the message, which result in the domination of either danger control (i.e., cognitive processes) or fear control processes (i.e., emotional processes)." The dominant mediator, which usually emerges from the two or several representative variables/mediators in the parallel process, is the determinant factor in the behavioral outcome. Initially, Witte (1995) proposed a formula[1] to describe the influence of the critical point between danger control logic and fear control logic in determining individuals' responses to threats. Later, Chen et al. (2021) proposed the enhanced formula[2] and systematically described and explained the relative weight between the danger control logic and fear control logic on employees' responses to ISec policy compliance.

However, the current discussion of treatment of the discriminant formula (Witte 1995; Chen et al., 2021) is problematic. From the standpoint of methodology, prior studies based on the EPPM theory (e.g., Witte 1992, Witte 1994, Chen et al., 2021) have assessed behaviors in individuals dominated by either fear control or danger control responses, using the discriminant value formula. This means classifying the individuals into fear control process groups or danger control process groups based on the standardized score of two constructs' measures (perceived threat and perceived efficacy; Witte 1995 and Witte et al.

* Corresponding author.
E-mail address: Yitian.Xie@xjtlu.edu.cn (Y. Xie).

[1] Discriminant value = (z score of perceived efficacy – z score of perceived threat)

[2] Discriminant value = ($\beta 1$ Z score of perceived efficacy — $\beta 2$ Z score of fear), where $\beta 1$ and $\beta 2$ are obtained from two simple regression lines: Protection motivation = $\beta 1$ x perceived efficacy, and Protection motivation = $\beta 2$ x fear.

https://doi.org/10.1016/j.cose.2024.103776
Received 16 August 2023; Received in revised form 6 February 2024; Accepted 15 February 2024
Available online 17 February 2024

1996, and perceived efficacy and fear; Chen et al., 2021) and testing the behavior of these groups separately. Unfortunately, this method raises two concerns. First, we argue, it neglects the impact of other factors (e.g., tenure of use) on individuals' engagement in problem-focused or emotion-focused responses. Second, as argued in this paper, it omits assessing the relative influence of mediators (such as fear, perceived threat, perceived efficacy) on the behavior of the entire sample. It is important for future research and application of the dominant mediator in EPPM to recognize these concerns regarding sample categorization based on the discriminant formula proposed by Witte (1995) and enhanced by Chen et al. (2021).

The objective of this paper is to introduce these two concerns and take a first step towards addressing them. As for the second concern related to the discriminant formula (Witte 1995; Chen et al., 2021), we propose testing of fear-appeal models with a dominant mediator with the multiple mediation model testing approach. This approach has three main advantages. First, the likelihood of parameter bias, due to omitted variables, is reduced as compared to the discriminant value assessment. Namely, while individuals have a dominant behavior, their behavior is still influenced by other mediators, and critical point assumption testing enables testing the combined effect of the mediators (i.e., the indirect effect of specific mediators conditionally on the presence of other mediators) on the whole sample's behavior. Second, testing the dominant mediator enables researchers to test hypotheses concerning the whole sample without creating different groups and testing their behaviors separately. Third, it allows researchers to provide empirical evidence related to how the relative weight of the mediators would influence coping responses (e.g., message acceptance or rejection).

Furthermore, as for the first concern of omitting the impact of other factors (e.g., tenure of use), the relative weight of fear and perceived efficacy in determining whether home users' actively use intention of anti-malware software hasn't been studied based on experienced users with different usage tenures of household anti-malware software.

To investigate this issue, we conducted an empirical study to test our research question: Which factor is dominant in determining experienced users' intention to actively use anti-malware software in their household computer(s)?

The contribution of the study is two-fold. First, this research is the first study to provide evidence for the dominant mediating role of perceived efficacy as compared to fear in an ISec context using the multiple mediation method. A statistically significant difference between fear and perceived efficacy was found in our empirical study of users' intention to actively use anti-malware software in their household computer(s). Specifically, perceived efficacy is found to be significantly higher than fear, leading to a positive behavioral outcome (i.e., actively using household anti-malware software). Second, we highlight the methodological benefits of testing the dominant mediator using multiple mediation model testing approach compared to the discriminant value equation introduced by Witte (1995), Witte et al. (1996) and enhanced by Chen et al. (2021).

2. Research background

The theoretical origins and statistical interpretation of dominant mediator assumption will be introduced in this section. First, Section 2.1. introduces the theoretical origins of dominant mediator assumption and the *contrast* hypothesis. Then, Section 2.2. explains the statistical interpretation of dominant mediator assumption and the contrast hypothesis in multiple mediation analysis.

2.1. The theoretical origins of dominant mediator

The dominant mediator assumption has a long history and can be initially traced to several pioneer fear appeal theories.[3] First, in Leventhal's (1970, 1971) Parallel Response Model (PRM), he noted that threat-induced appraisals can induce two parallel responses. One is danger control process, which refers to the attempts to solve the threat-induced problem (Leventhal 1970, 1971). The other is fear control process, which refers to the efforts put in to deal with one's negative feelings (e.g., fear, anxiety, worrying) regarding specific threats (Leventhal 1970, 1971). To give an example in ISec context, individuals may have read a newspaper about a type of ransomware that emerged recently that may lock their computers and cause financial loss of their credit cards. When they realize there's an effective and handy anti-malware software to avoid the potential damage caused by ransomware, they may consider enhancing their security posture by actively using the anti-malware software. For instance, they may scan for suspicious software every time before downloading documents from the internet. In this case, they are engaging in a cognitive control logic. On the contrary, when they suspect the effectiveness of the anti-malware software, and their doubts regarding the effectiveness of the countermeasures may outweigh their beliefs regarding the effectiveness of the protection, they may engage in a variety of fear control process logic. In this case, an emotion control logic may be dominant, and maladaptive responses may occur. They may ignore the security notifications, deny the severity of ransomware, downplay the possibility that certain accidents could happen to them, or repress thoughts about the threat.

Later, Rogers (1975) proposed PMT, and in 1983, he further proposed the revised PMT (Maddux and Rogers, 1983), both are well-known in ISec (Boss et al., 2015; Siponen et al., 2023). What is less known in ISec that Rogers (1975), Maddux and Rogers (1983) criticized the ambiguous theoretical proposition and testing in PRM (Leventhal 1970, 1971). He highlighted a need for a more precise and unequivocal connection between the theoretical background and the hypothesis (Rogers 1975), Maddux and Rogers (1983). Specifically, a clarified hypothesis and test of the parallel process (e.g., the relative magnitudes of the mediators) may contribute to a better theoretical explanation of the behavior outcome. As Rogers (1975) notes:

A second inadequacy of the [Leventhal's] parallel response model [PRM] is that the logical relationships of the constructs are not sufficiently precise to generate unequivocal hypotheses. While an assumption of the independence of the danger and fear control processes may predict an independence of verbal, physiological and overt behavioral measures, as Leventhal suggests, it is doubtful that many of the 'predictions' are derivable from the model (p. 108).

Later, Witte (1992) also criticized Leventhal's (1970, 1971) PRM and made propositions of different behavioral outcomes derived from the different relative weights of mediators. As Witte (1992) noted, PRM "made general statements about conditions leading to fear or danger control process, but [PRM] failed to specify exactly when one process should dominate over another or what specific factors elicit the different process" (p. 333).

The above argument stated a need to establish an unequivocal theoretical explanation/prediction of how the relative weight of the mediator will influence behavioral outcomes. However, the empirical method, called the discriminant value formula, proposed by Witte (1995, p. 239), tested in Witte et al. (1996, p. 321), and enhanced by Chen et al., 11) predicts behavioral engagement based *only on two* constructs. Therefore, it contains certain shortcomings. For example, the formula neglects the effect of other important factors and tests the behavior of persons engaging in fear control and danger control processes separately.

To this end, we propose to test the dominant mediator assumption in fear appeal studies using *contrast* (i.e. *the contrast of the two mediators*) to statistically determine the relative weight of the mediators in a multiple mediation model instead of using the discriminant value method by

[3] For detailed information, see Appendix 2.

Witte (1995), Witte et al. (1996), and Chen et al. (2021).

2.2. The statistical methods for the dominant mediator

In this subsection, we give a short overview of the multiple mediator models and the test of contrast. Multiple mediator models refer to models involving multiple simultaneous mediators (Preacher and Hayes, 2008). As an illustrative example, Fig. 1 depicts a multiple mediator model with *n* mediators. Multiple mediator models enable testing the indirect effect of specific mediators conditionally on the presence of other mediators in the model. This is important in fear-appeal models when multiple mediators (both the emotional valence factors, like fear, and the cognitive valence factors, such as perceived efficacy) simultaneously affect behavioral outcome. Next, we introduce the concept of *Contrast* (Preacher and Hayes, 2008) as a measure to examine the statistical differences between the two specific indirect effects.

Comparing the relative weight of the core mediators in the EPPM by quantifying the contrast between two indirect effects has several advantages. First, by calculating and reporting the *contrast*[4] metric, the theoretical propositions of the relative weight of the IVs-MEs-DVs relationship can be elucidated (Preacher and Hayes, 2008). Furthermore, researchers can reveal if there is a statistically significant difference between the two mediators (Preacher and Hayes, 2008). Moreover, researchers could recognize when one process dominates over another or different combinations of mediators with different weights may elicit certain behavioral processes. In another word, researchers can identify the "when" condition(s) which leads to certain coping responses (or the boundary condition of the theory model) (Busse et al., 2017; Davison and Martinsons, 2016; Hong et al., 2014). Specifically, for empirical studies based on EPPM, dominant mediator assumption can help to determine the behavioral outcome (either as danger control process or emotion-focused coping) by measuring the relative weight of the danger control process and the fear control process. With dominant mediator assumption, researchers can determine, for example, that the response efficacy appraisal should be significantly higher than the response cost appraisal and, thus, lead to danger control process. Otherwise, it may lead to emotion-based copings (see Appendix 3.2).

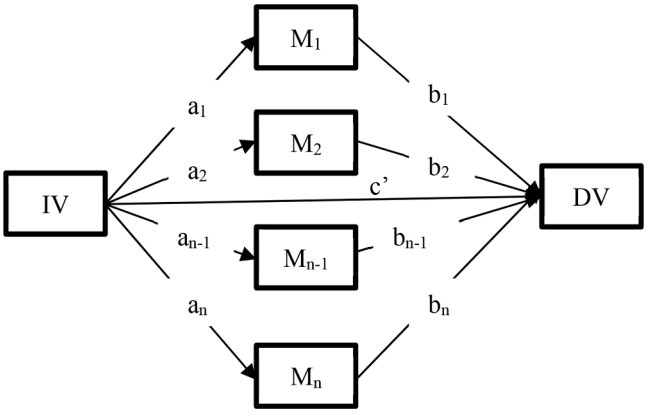

Fig. 1. Illustration of a multiple mediation design with *n* mediators
Note: *IV* is hypothesized to exert indirect effects on *DV* through M_1, M_2, …, M_n. All of these paths (e.g., a_1, b_1, c') are quantified with unstandardized regression coefficients.

[4] To address the importance of the relative weight of the mediators (e.g., contrast perceived efficacy with fear), in this paper, we use the product-of-coefficients and bootstrapping methods to test hypotheses about *contrasts* (Preacher and Hayes, 2008).

3. Conceptual background and hypotheses development

This section draws the key constructs and propositions in the extended parallel process model (EPPM) (Witte, 1992, 1994; 1996) as a theoretical foundation for our empirical study. We modified and contextualized the EPPM to harmonize it with our research context (i.e., experienced users intend to use anti-malware software on their home computers actively) and proposed our research hypotheses based on the adjusted model. Moreover, we elucidated the conceptual definition of the dominant mediation.

3.1. Conceptual background

According to Witte (1996, p. 428), "[*t*]he EPPM integrates and expands on previous perspectives to explain when and why fear appeals work and when and why they fail".

Fig. 2 shows an adjusted EPPM model in the context of household anti-malware software usage among experienced users. The adjusted EPPM was established based on several key theoretical constructs and propositions in EPPM (Witte 1992, 1994), with an overview of the hypotheses delineated in 3.2.

Threat

The first key construct in EPPM (Witte 1992, 1994; 1996) is threat. And there's a difference in the definition between threat and perceived threat. According to Witte et al. (1996 p.320), "[a] threat is a danger or harm in the environment whether we know it or not," while "[*p*]erceived threat is cognitions or thoughts about that danger or harm." To illustrate it with an example, a keylogger is a threat because it can collect user keystrokes without their awareness. The perceived threat of a keylogger is the cognitions or thoughts about potential damages, such as a data breach, caused by monitoring keystrokes.

Efficacy

The second essential construct in EPPM (Witte 1992, 1994; 1996) is efficacy. Witte (1996, p. 429) states, "[*e*]fficacy pertains to the effectiveness, feasibility, and ease with which a recommended response impedes or averts a threat", while "[*p*]erceived efficacy is thoughts or cognitions about the effectiveness of the recommended response in deterring the threat" (Witte et al., 1996, p.320). For example, users perceived the functionality of the installed anti-malware software could detect and delete a keylogger.

Fear

The third important factor proposed in EPPM (Witte 1992, 1994; 1996) is fear. Witte (1996, p. 429) states, "[*f*]ear is an internal emotional reaction composed of psychological and physiological dimensions that may be aroused when serious and personally relevant threat is perceived." Fear of malware threats warning, different from fear of health threats (e.g., warnings of the coronavirus) or natural hazards (e.g., warnings of a nearby earthquake), can only be generated when individuals perceive a malware threat could cause severe and personal-relevant consequences. To exemplify it, fear may be raised when notifying the potential password leaking of a sensitive and important website (e.g., a bank account). Instead, possible password leaking on a marketing-purposes-only website may not raise much concern.

Continued Use Intention

Continued use intention is seen as an intention resulting from a rational decision to continue using the technology based on beliefs about, expectations of, or experience with that technology (Ortiz de Guina and Markus 2009; Bhattacherjee and Lin 2015). Continued use intention is positively associated with the continued planned behaviors or the intended actions (Warkentin et al., 2016a). Unlike continuance behavior, continued use intention is based on conscious choice that is less influenced by extraneous circumstances (Warkentin et al., 2016a). Users may have their evaluation of specific IT in the post-adaptive stage (Bhattacherjee and Lin 2015). For example, after the users have gained experience with the security technology, they may form a belief about

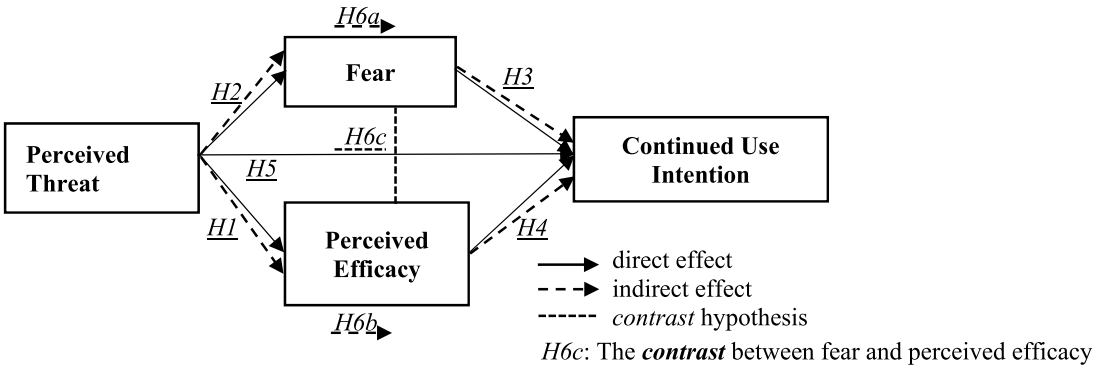

Fig. 2. Proposed Conceptual Model.

the efficacy of the product, and they may rely heavily on their own assessments regarding the decision to continue or cease to use it (Warkentin et al., 2016a; Vedadi and Warkentin, 2018, 2020).

Dominant Mediator

Dominant mediation depicts the relative magnitude of specific indirect effects in a multiple mediation model. If one specific indirect effect is significantly higher than the others, it becomes the dominant mediator among all the mediators. The dominant mediator can facilitate the elaboration of the theoretical explanations of dominant coping logic in EPPM. In addition, the dominant mediator can be hypothesized as a contrast between two indirect effects and tested by a multiple mediation model (Preacher and Hayes, 2008). Witte (1995) and Witte et al. (1996) proposed and tested the dominant mediator as a key proposition in EPPM, and it was further developed and tested by Chen et al. (2021). Witte et al. (1996, p. 321) state, "[*t*]he critical point occurs when perceptions of threat begin to outweigh perceptions of efficacy, causing people to shift from danger control to fear control processes". Similarly, Chen et al. (2021) proposed that a danger control process (e.g., security message acceptance) may occur when perceived efficacy outweighs fear. Instead, when fear dominates, a fear control process (e.g., security message rejection or no response) will occur.

3.2. Conceptual model and hypothesis development

In this section, we propose a conceptual model based on key elements and propositions in EPPM and contextualize it among experienced anti-malware software users. Furthermore, we develop the hypothesis of the dominant mediator (i.e., the contrast hypothesis) in our study context.

We proposed perceived threat as the independent variable (IV), continued use of anti-malware software as the dependent variable (DV), and fear and perceived efficacy as two mediators (Me). Since regard the perceived threat as IV and the fear as a mediator are consistent with both the theoretical propositions in EPPM (Witte 1992, 1994) and seminal empirical studies related to EPPM in the ISec field (Boss et al., 2015; Lowry et al., 2023; Moody et al., 2018), we devote most of our effort into explaining the reason why we chose perceived efficacy as a mediator.

We need to develop our mediation model based on the theoretical foundation and the contextualized reasoning of the temporal presence of the variables (Pirlott and MacKinnon, 2016). Our proposed model is based on the temporal precedence of perceived threat over perceived efficacy (and fear). Specifically, we proposed perceived efficacy as a mediator for two reasons. It is based on 1) a consideration of the theoretical basis, and 2) a methodological consideration of the mediation model development.

First, in EPPM (and most other fear appeal studies), an assessment of perceived efficacy (as second appraisal) is often followed by exposure to and perceived a threat (as the first appraisal) (Witte 1992, 1994). Following this idea, perceived threat occupied a precedence position over perceived efficacy, which is theoretically justifiable per Witte (1994).

Second, perceived threat occupied a precedence position over perceived efficacy in the context of continued use of anti-malware among experienced users. Perceived efficacy reflects how much control users believe over the threat by using a safeguard. Therefore, awareness and admitting a severe and personally relevant malware threat (i.e., perceived threat) is usually a premise. Thus, the temporal precedence of perceived threat gets legitimacy support for the proposed model (Pirlott and MacKinnon, 2016).

Perception of a malware threat is the premise of the perception of the efficacy of an anti-malware software (Warkentin et al., 2016a Xie et al., 2022). Users may raise a positive feeling toward the installed security protection since it helped them successfully avoid malware threats (Safa et al., 2015). One example is that anti-malware software users learn that their neighbor encountered a privacy intrusion because of keyloggers. It was stealthily installed in victims' household computers, and sensitive information was stolen for financial purposes. In this case, once users perceive the threat (i.e., keyloggers) as severe and also relevant to themselves, they may recognize the value of anti-malware software, realizing that similar threats could attack them if they do not have effective protection. Therefore, we hypothesis:

Hypothesis 1: *Perceived threat positively associated with perceived efficacy.*

Fear may be aroused when individuals perceive a severe and personally relevant threat (Witte 1992, 1994; 1996). In anti-malware software use, fear could be aroused by an awareness of potential financial loss, sensitive information breaches, and privacy hazards caused by malware (Boss et al., 2015; Liang et al., 2019). Experienced anti-malware software users, aware of the severe consequences of various potential malware threats (such as new types of malware, botnets, and zero-day attacks), may increasingly experience adverse emotional reactions, including worries or concerns about potential losses due to these hazards (Boss et al., 2015; Liang et al., 2019). Therefore, we hypothesize:

Hypothesis 2: *Perceived threat positively associated with fear.*

Fear is an adverse emotional arousal toward a threat's potential damage and manifests as anxiety and worry over the possible loss (Aurigemma and Mattson, 2018; Moody et al., 2018). For example, users learned that malware could cause the malfunctioning of someone's personal computer; spyware can lead to data breaches and compromise users' privacy and cybersecurity; ransomware may lock users' important files, leading to financial loss. These consequences may impair their work performance and even lead he/her lose their jobs. The fear or concern towards malware threats drives users to pursue ways to avoid malware threats. Therefore, we hypothesize:

Hypothesis 3: *Fear positively associated with continued use intention to actively use household anti-malware software.*

Users' beliefs in the effectiveness of their responses will shape how they react to the threat. Response efficacy is linked with positive attitudes towards mitigating the threat, influencing how they implement

the recommended responses. Users are inclined to develop a disposition regarding their future behavior, either ceasing to use or actively employing anti-malware software, based on their evaluation and confirmation of the software's protective capabilities (Martens et al., 2019; Safa et al., 2015;Warkentin et al., 2016a ; Xie et al., 2022). Users are more likely to actively use anti-malware software when they recognize its functionality and effectiveness. For instance, if users believe that worms can be identified and isolated promptly by keeping their anti-malware software open and updating it with the latest patches, they are more likely to regularly use and update their software. Therefore, we hypothesize that:

Hypothesis 4: *Perceived efficacy positively associated with continued use intention to actively use household anti-malware software.*

The perceived existence of malware threats is necessary to continue using anti-malware software (Warkentin et al., 2016a; Xie et al., 2022). As the perception of threats intensifies, individuals become more motivated to continue actively using anti-malware software on their household computers to avoid potential damage from malware. Research has shown that perceived threats correlate positively with the continued use of anti-malware software, particularly when the threats pose severe and personally relevant damage (Warkentin et al., 2016a; Xie et al., 2022). In contrast, perceiving a threat as insignificant may lead to the cessation or reduced use of anti-malware software protection. For example, ransomware attacks involve encrypting a device's data and holding it for ransom, with the threat actor threatening to delete or release valuable data if the ransom isn't paid by a specific deadline. When users are aware of the severe potential losses caused by ransomware, they are more likely to actively use their household anti-malware software to prevent such attacks. Therefore, we hypothesize:

Hypothesis 5: *Perceived threat positively associated with continued use intention to actively use household anti-malware software.*

When users are aware of severe and personally relevant threats, they may become worried or anxious about the potential losses these threats can cause. This intense negative emotion motivates them to take action, such as scanning documents before downloading to avoid virus infection. For instance, awareness that spyware can lead to the theft of sensitive credentials, potentially resulting in privacy breaches and financial losses, may heighten users' anxiety when downloading suspicious files. This worry or anxiety then prompts them to actively use their household anti-malware software as a precaution against potential spyware-induced losses. In this context, fear acts as a catalyst, motivating users to consistently and actively engage with their anti-malware software. Therefore, we hypothesize that:

Hypothesis 6a: *Fear mediates the relationship between perceived threat and continued intention to actively use household anti-malware software.*

The appraisal of response efficacy is a cognitive process where individuals assess the effectiveness of a recommended response in averting a threat, as outlined by Rogers (1975), Maddux and Rogers (1983) and Witte (1992, 1994). When users recognize a threat as both severe and personally relevant, they initiate a cognitive evaluation of how effective the recommended responses might be. The stronger their belief in the efficacy of these responses, the more motivated they become to implement them. For instance, consider a user who becomes aware that malware can corrupt or delete crucial computer data and files. Upon learning that regular, comprehensive scans and timely updates of antivirus definitions can effectively prevent the damaging consequences of malware infections, they may begin to use features of their anti-malware software more actively, such as keeping it running and updating it with new patches promptly. Therefore, we hypothesize:

Hypothesis 6b: *Perceived efficacy mediates the relationship between perceived threat and continued intention to actively use household anti-malware software.*

While anti-malware software is a handy and effective tool to identify and avoid most malware, it does not guarantee perfect protection against all malware threats.[5] This implies that some users may doubt that an anti-malware product can be the best way to mitigate threats and be worrying about it, although they are aware that anti-malware software provides certain functionalities to protect their home computers. In this case, fear and perceived efficacy are essential factors in the parallel emotional and cognitive appraisal process model. More importantly, the relative weight between fear and perceived efficacy[6] may induce different coping responses in users. Unlike some scenarios in the health context, it is rare for experienced users to reach a high level of fear when using anti-malware software in daily scenarios. Instead, users may experience only moderate to low levels of worry about potential malware threats (Siponen et al., 2023). This negative emotion usually facilitates users to focus on problem-focus logic, as several previous studies report (e.g., Boss et al., 2015; Chen et al., 2021; Liang et al., 2019; Posey et al., 2011). Therefore, we hypothesize:

Hypothesis 6c: *There is a significant difference between the two mediators (*i.e.*, perceived efficacy and fear) in contribution to the IV-DV relationship (*i.e.*, perceived threat->continued use intention), while one mediator (*i.e.*, perceived efficacy) outweighs the other (*i.e.*, fear).*

4. Research method

A cross-sectional designed study is applied to test the research model. In the following section, we discuss the survey instrument and the data collection process.

4.1. Data collection

The data were collected from a Qualtrics, LLC panel of 502 adults from the United States. We recruited full-time workers who had anti-malware use experience of more than one year on their home computer(s). Participants took an online survey (www. Qualtrics.com) that was used to investigate individuals' perceptions of home information security and continued use intention in regard to the anti-malware application(s) on their home computer(s).

To test the hypothesized relationships, measures were adopted from the literature and modified to assess the constructs described in the research model. Appendix 1 shows the measurement items, the source of the items, and the demographic questions. To counteract the possibility of careless responses, three statements were provided, including the following: "For this question, only answer 3, somewhat disagree; do not give any other answer." The responses that did not correctly answer these scrutiny questions were screened out as careless responses. All 502 responses we received from Qualtrics passed this criterion screening

[5] Most modern anti-malware programs are based on a database of virus signatures composed of previously identified malware while limited in other protection functions. When new malware is discovered, it is sent to the anti-malware company, and the malware's digital signature or hash is created and added to the database. This means that there is a vulnerable time frame between the creation of new malware and the updating of antivirus program databases. During this period, malware can (and has) caused significant havoc.

[6] An alternative situation could be that the users' belief in the effectiveness of anti-malware software to avoid malware threats is low. As a result, the users may stop using anti-malware software. Instead of relying on signature-detection-based anti-malware software, they may use manual ways to detect malware threats (e.g., have a whitelisted database of suitable processes and monitor changes on the HDD/SSD). Or even worse, they use emotion-focused coping responses to improve their anxiety towards malware threats.

check.

4.2. Sampling strategy and sample characteristics

Firstly, a purposeful sampling strategy (Kelly, 2010; Robinson, 2014) was applied in the data collection process. The inclusion and exclusion criteria are listed below. The inclusion criteria for this study required participants to be household anti-malware software users in the US with over one year of experience. This ensured that the opinions gathered came from experienced users familiar with a variety of situations and scenarios in the household context. The study excluded individuals who either did not install anti-malware software on their household computer(s) or had less than one year of usage experience. Having defined these key characteristics, we obtained a refined sample pool of long-term household anti-malware users (more than one year). We then conducted the data collection process using random sampling within this refined pool.

The details of the demographic information of the respondents are shown in Table 1. The sample size ($n = 502$) is sufficient for testing the covariance-based structural equation model with the maximum likelihood (ML) algorithm (Jackson, 2003) to detect the mediation effect (Fritz and MacKinnon 2007) and the decomposition effect of the mediation analysis (Fairchild et al., 2009). After the final model runs, we applied a few control variables *ex post facto* to check the completeness of our model for model fit.

4.3. Common method bias

We conducted both procedural control and statistical remedies for potential common-method bias (CMB) (Podsakoff et al., 2012). For procedural control, we took the following proactive steps. First, we used anonymous statements in the survey instrument to reduce social desirability bias. Second, we counterbalanced the order of all the questions. Third, we used the attention checks techniques to make sure that the participants paid careful attention to their responses, such as "For this question only answer 5, somewhat disagree; do not give any other answer." We also employed a marker variable technique (Williams et al., 2010) to assess common method bias (CMB). Individual-collectivism was considered as the marker variable. We compared the structural model with and without this marker variable. Our analysis revealed no statistically significant correlation between the marker variable and the principal constructs of the model. Additionally, the path coefficients remained unchanged with the inclusion of the marker variable. Therefore, we concluded that CMB was not a significant concern in our study.

Table 1
Demographics of respondents.

Characteristic	Frequency	Percent (%)
Gender		
Male	251	50 %
Female	251	50 %
Age		
18–30	59	12 %
31–40	81	16 %
41–50	108	22 %
51–60	141	28 %
Above 60	112	22 %
Not Report	1	0
IT-related work		
IT-related	56	11 %
Non-IT-related	446	89 %

5. Data analysis and model estimation results

5.1. Measurement model analysis

The data were calculated with SPSS 24.0 and Amos 24.0.[7] The report of scale reliability and validity followed Gefen et al. (2011). The means, standard deviations, factor loadings, and squared multiple correlations (SMC) are reported in Table 2. Survey questions are in Appendix. The results showed that the scale achieved good reliability and validity.

Furthermore, we used the square root of the AVE values and latent variable correlations to evaluate discriminant validity. Good discriminant validity requires the AVE value's square root for each variable to be higher than the correlations between that and all other variables. Table 3 shows that our dataset has adequate discriminant validity. We further conducted a discriminant validity test using the heterotrait-monotrait (HTMT) ratio of correlations criteria (Henseler et al., 2015). The HTMT ratios presented in Table 4 are all below the threshold value of 0.85, indicating that our dataset did not have discriminant validity problems.

5.2. Structural model analysis

The covariance-based structural equation modeling followed the procedure suggested by Kline (2023). We performed a chi-square test on the measurement model and the structural model and heuristically used the goodness-of-fit index to evaluate the quality of the proposed model. The results of the goodness-of-fit index check show that all the indicators achieved good model fit (see Table 5). All path coefficients achieved statistical significance in our model (see Table 7). Hence, the results showed strong support for H1-H5.

(GFI: goodness-of-fit indices; CFI: comparative fit index; NFI: normed fit index; SRMR: standardized root mean square residual; and RMSEA: root-mean-squared error of approximation.)

5.3. Mediation analysis

Next, we performed a *percentile-based* bootstrap confidence interval (CI) and a *bias-corrected* (BC) bootstrapping CI with 5000 iterations to examine the specific indirect effect of the mediators and the relative weight of them. (Hayes, 2009; Preacher and Hayes, 2008; Zhao et al., 2010). The results (Table 6) confirmed the existence of partial mediation effect for perceived threat in fear (mediation effect = 0.038) and perceived efficacy (mediation effect = 0.172). The standard error (*SE*), critical ratios, and percentile-based bootstrap CI for these effects are reported in Table 6. These results support the mediation assumption (indirect effect) in H6a and H6b. Furthermore, as shown in Table 6, the difference in specific indirect effects showed that the mediation effect size of perceived efficacy outweighs fear and the difference is statistically significant (0.133, $p = 0.004$). Therefore, the H6c is also supported.

The results show that the mediators fear and perceived efficacy partially mediate the continued use of anti-malware software. Perceived threat induces both fear and perceived efficacy; however, the impact of perceived threat on fear is greater than its impact on perceived efficacy. However, fear does not affect the intention to continue using anti-malware software as much as the perceived efficacy. Furthermore, the direct effect of perceived threat on the continued use of antimalware software is more dominant than the specific indirect effects, and the total indirect effect of the mediators.

5.4. Control variables

We consider several control variables to reduce the potential of

[7] The decomposition effect of mediation analysis is estimated by user-defined syntax (Arbuckle 2013).

Table 2
Measurement Model Analysis.

Construct	Items	Means	SD	Factor loadings	Squared multiple correlation (SMC)	Coefficient alpha	CR
Perceived Threat (PT)	PT1	5.75	0.066	0.716	0.757	0.866	0.776
	PT2	4.8	0.079	0.699	0.534		
	PT3	5.71	0.063	0.816	0.883		
Perceived efficacy (PE)	efficacy1	5.74	0.052	0.831	0.868	0.931	0.867
	efficacy2	5.55	0.049	0.723	0.809		
	efficacy3	5.84	0.049	0.699	0.804		
Continued use intention (CONT)	cont1	5.07	0.083	0.743	0.912	0.967	0.965
	cont2	5.18	0.081	0.723	0.969		
	cont3	5.13	0.081	0.767	0.965		
Fear (FEAR)	FEAR1	2.91	0.078	0.881	0.726	0.711	0.825
	FEAR2	2.67	0.075	0.934	0.815		
	FEAR3	2.9	0.073	0.895	0.802		

Table 3
The square root of the AVE and the latent variable correlation.

	Threat	Fear	Efficacy	CONT	The square root of the AVE
Threat	**0.556**				0.746
Fear	0.246	**0.817**			0.817
Efficacy	0.480	0.118	**0.567**		0.753
CONT	0.435	0.191	0.419	**0.554**	0.744

Table 4
HTMT results.

	Threat	Fear	Efficacy	CONT
Threat	–			
Fear	0.249	–		
Efficacy	0.437	0.191	–	
CONT	0.485	0.203	0.419	–

Table 5
Model fit.

Fit index	Recommended value	Measurement model	Structural model
x^2	–	92.231	94.261
df	–	48	49
x^2/df	≤ 3	1.921	1.924
GFI	≥0.90	0.989	0.961
CFI	≥0.92	0.992	0.992
NFI	≥0.90	0.983	0.983
SRMR	≤0.08	0.057	0.061
RMSEA	≤0.08	0.026	0.026

Table 6
Mediation analysis.

Point Estimate	Product of Coefficients		Bootstrapping			
			BC 95 % CI		Percentile 95 % CI	
	SE	*Z*	Lower	Upper	Lower	Upper
Total effect						
0.639	0.068	9.397	0.552	0.777	0.519	0.749
Direct effect						
0.429	0.088	4.875	0.306	0.596	0.265	0.552
Total indirect effect						
0.210	0.048	4.375	0.146	0.302	0.145	0.301
Specific indirect effect						
PT–>PE–>CONT						
0.172	0.046	3.739	0.111	0.260	0.111	0.257
PT–>Fear–>CONT						
0.038	0.012	3.167	0.022	0.062	0.020	0.059
Contrast (PE vs. Fear)						
0.133	0.046	2.891	0.068	0.218	0.068	0.218

Note: BC, bias-corrected; CI, confidence interval; 5000 bootstrap samples.

Table 7
Results of the Structural Model Assessment.

Hypothesis	Path Coefficient (p-value)	Support?
H1: PT -> PE	0.370 (0.000)	Supported
H2: PT -> FEAR	0.306 (0.000)	Supported
H3: FEAR -> CONT	0.061 (0.000)	Supported
H4: EFFICACY -> CONT	0.317 (0.000)	Supported
H5: PT -> CONT	0.338 (0.000)	Supported
Mediation Hypothesis		
H6a: PT -> FEAR -> CONT	- (see Table 6)	Supported
H6b: PT -> PE -> CONT	- (see Table 6)	Supported
H6c: contrast of FEAR and PE	- (see Table 6)	Supported
$\mathbf{R^2}$ FEAR	0.084	
EFFICACY	0.268	
CONT	0.393	

Note: Bolded p-values are significant (< 0.05).

omitted variable bias (Angrist and Pischke, 2009). Prior work suggests that various characteristics of a person affect how (s)he perceives threat, fear, and efficacy, and also affect their continued use intention to use household anti-malware software actively. These characteristics are the following: *age* (Boss et al., 2015; Johnston and Warkentin, 2010), *gender* (Boss et al., 2015; Johnston and Warkentin, 2010), *education* (Boss et al., 2015; Johnston et al., 2015), *work experience* (Boss et al., 2015; Johnston and Warkentin, 2010), *work type* (i.e., work at IT-related position or not), *computer use experience* (Boss et al., 2015). Based on the suggestions of previous studies, we controlled for these variables in our study.

6. Discussion

In this section, we discuss 1) the main findings of this study compared with the previous studies, 2) the theoretical and methodological contribution of testing the dominant mediation assumption, and 3) the practical suggestions for message design for security notifications.

6.1. Findings

In this study, we examined the direct effect of perceived threat on cognitive appraisal, emotional appraisals, and continuous behavioral intention; the indirect effect of fear and perceived efficacy between perceived threat and continued use intention; and the contrasting effect between fear and perceived efficacy. We contribute to existing knowledge in the following ways.

First, we found support for the influence of perceived threat on perceived efficacy (***H1***). This finding supports the classic view of EPPM (Witte, 1992; Chen et al., 2021) in the context of the post-adaptive intention of household anti-malware software. That is, the perceived threat occupies a precedence position over perceived efficacy in message processing. Specifically, we discovered that perceived threat (as a key construct of the first appraisal) significantly influences the perceived efficacy (as a key construct of the second appraisal) when processing

security messages in the post-adaptive stage of anti-malware software.

Second, while previous studies show inconsistent results regarding the influence of perceived efficacy on fear, our study supports a positive impact of perceived threat on fear (***H2***). Some studies provide support for the influence of perceived efficacy on fear (e.g., Boss et al., 2015; Chen et al., 2021; Moody et al., 2018), while others indicate that perceived threat does not play a significant role in fear (e.g., Posey et al., 2011). In this study, we provide empirical evidence that perceived malware threats could lead to a feeling of fear among experienced users in the post-adaptive use of anti-malware software.

Third, while previous studies show inconsistent results regarding the influence of fear on protection motivation behavior, our results support the hypothesis of FEAR-CONT (***H3)***. Some studies provide support for the significant impact of fear on protection motivation behavior (e.g., Moody et al., 2018; Lowry et al., 2023), while others show that fear does not play a significant role in motivating individuals to engage in protection motivation behaviors (e.g., Boss et al., 2015; Chen et al., 2021; Posey et al., 2011). In this study, we provide empirical evidence that fear of malware threats could motivate users to continue using intention of anti-malware software.

Fourth, we found support for the PE-CONT (***H4***) and PT-CONT (***H5)*** hypothesis. These results are consistent with previous empirical studies based on the EPPM (e.g., Boss et al., 2015; Warkentin et al., 2016a).

Fifth, our mediation results support hypotheses 6a (***H6a***) and hypotheses 6b (***H6b***), which indicate that both the negative emotional valence (fear) and the positive cognitive valence (perceived efficacy) can mediate the relationship between perceived malware threat and continued use intention of household anti-malware software. These results offer empirical evidence regarding the mediation role of FEAR and PT between PE and CONT among experienced home users.

Sixth, we found support for the contrasting effect of the two mediators supports hypothesis 6c (***H6c***), which explains that perceived efficacy is a more dominant factor triggering a danger control process mechanism than fear. In other words, once users are aware of the severity and personal-relevant malware threat, when perceived efficacy outweighs the fear, they continue to actively use anti-malware software on their household computers. This is the first study that empirically confirms the contrasting relationship between fear and perceived efficacy in a multiple mediation model approach. We extend existing findings by confirming the theoretical proposition of "contrast" in EPPM (Witte 1992, 1994), which assumes that the relative magnitude difference between fear and perceived efficacy statistically significantly influences the continuance of protection motivation behavior.

6.2. Research implications

Our paper makes two major contributions. First, we draw the ISec community's attention to the potential merits of testing the dominant mediator assumption in fear-appeal studies through multi-mediation testing, as opposed to using the discriminant formula introduced by Witte (1995, p. 239), and enhanced by Chen et al., p.11). Testing the dominant mediator assumption with multiple mediation testing allows to contrast mediators (e.g., fear and perceived efficacy) and compare their indirect effects on the behavioral outcome to not only identify which mediator is active but also determine which process or mechanism is stronger or more dominant. Fear appeal scholars have argued that the failure to specify under which circumstances danger control process or fear control process is dominant is an important limitation of the theoretical implication of the fear appeal model (Rogers 1975; Witte, 1992, 1994). This research is the first study to provide evidence for the dominant mediating role of perceived efficacy as compared to fear in an ISec context using multiple mediation method. Specifically, our study is the first study to demonstrate that as experienced home users are notified of a highly damaging and personal-relevant threat to their home computer(s), they will intend to continue to actively use anti-malware software as long as their confidence in the utility of the technology in protecting their information assets or system stability outweighs the fear of the threats.

Further, our study sheds new light on the validity of the enhanced discrimination value introduced by Witte (1995) and enhanced by Chen et al. (2021). They argue to discriminate individuals' behavior based on perceived efficacy and perceived threat (Witte, 1992, 1994 and 1996), and based on perceived efficacy and fear (Chen et al., 2021). In this paper, we argue against assessing an individual's engagement in emotion-focused logic or problem-focused logic based on the standardized score of only two constructs' measures (i.e., the constructs perceived efficacy and perceived threat in studies by Witte, 1992, 1994 and 1996; and the constructs perceived efficacy and fear in Chen et al., 2021) using two arguments. First, our results suggest that due to the significance of the direct and both indirect effects, individuals' behavior is affected by all three constructs (perceived threat, perceived efficacy, and fear). Second, our findings related to the dominant mediating role of perceived efficacy over fear emphasize the importance of perceived efficacy in determining behavioral outcome in ISec context, as opposed to perceived threat and fear as the enhanced formula introduced by Chen et al. (2021) suggests. Third, several other factors (e.g., age, gender, education, work experience) affect individual's behavior whose effects are neglected from the discriminant value equation, and they might cause omitted variables bias. We illustrate this with an example: Consider a person who scores the same on measures of perceived threat (i.e., fear of potential identity theft) and perceived efficacy (i.e., ability to prevent it by using strong passwords), regardless of whether the measurement is taken in the morning or evening. However, her actual behavior (i.e., the behavioral outcome) might differ based on her energy levels. She might opt for weak passwords in the evening due to fatigue, while preferring strong passwords in the morning when she is more energetic. Therefore, classifying her into emotion-focused or problem-focused groups based solely on her perceived threat and efficacy values, and hypothesizing and testing her danger control process or emotion-focused coping (i.e., whether she uses strong or weak passwords) based on this classification, could lead to biased results.

Second, our study questions the central role of fear in the EPPM theory (Witte, 1992)[8] in ISec context. While in EPPM fear is presented as a crucial factor, and EPPM clearly distinguishes between the danger-control and fear-control processes, in the empirical assessment of the theory Witte (1994) and Witte (1996) fear was not measured, and its effect was not tested. Instead, individuals were classified into danger-control and fear-control groups based on the standardized scores of perceived threat and perceived efficacy, and tested whether these groups respond differently (i.e., the danger-control group in adaptive, and the fear control group in a maladaptive manner). Thus, the assessment of EPPM theory presented in Witte (1994) and Witte (1996) does not provide evidence on the crucial role of fear on behavioral outcome. This aspect is not mentioned in the extant criticism in the fear debate in ISec (Chen et al., 2021; Siponen et al., 2023; Warkentin et al., 2016b). Based on the results of our study, and considering our concerns regarding the discriminant value formula mentioned above, we recommend that future ISec research reevaluates the strong distinction between fear control and danger control behaviors as suggested by the EPPM theory.

6.3. Practical implications

We provided practical instruction by testing and reporting the relative magnitudes of the specific indirect effects and the contrast between two indirect effects. Our findings indicate that security practitioners

[8] As noted by the title of Witte (1992), "Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Successes and Failures", fear has long played an essential role in determining the behavioral outcome in the EPPM.

should base the design of security notifications on theory to motivate active use of household anti-malware software. Specifically, anti-malware security notification designers should first make home users aware of threats they were unaware of before. The notifications can detail the severity and relevance of these threats. Then, more emphasis should be given to increasing the perception of coping efficacy to deal with the threat. Practical instruction and hands-on experience on how to deal with specific malware threats could be provided in security notifications. Most importantly, designers of anti-malware security notifications should aim to communicate in a manner that enhances users' perception of the efficacy of anti-malware protection and their own self-efficacy, thereby surpassing any fears or concerns they may have about potential malware threats.

Second, we shed light on the role of fear in the decision-making process among experienced household users. In the context of health research, the consequences of health-related threats can be lethal (Witte, 1992). As a result, affected individuals may experience high levels of fear and engage in maladaptive behaviors, such as denial, intentional ignorance, or downplaying the information. However, unlike in the health context, the fear of potential malware threats among experienced household anti-malware software users is more likely to manifest as a medium or low level of worry about possible loss. Fear, in the malware case, is more likely to act as a facilitator than a suppressor. In other words, experienced household users are more motivated by this medium or low level of worry and tend to adhere to the established security solutions to protect their information assets and household computer(s).

6.4. Limitations and future research directions

We report three limitations. First, the causality of the study can be limited because of the cross-sectional survey design (Bullock et al., 2010). Future studies with stronger causal settings are needed (Imai et al., 2011; Pirlott and MacKinnon, 2016; Shrout and Bolger, 2002). Second, the generalizability of the study can be limited because of the sample characteristics (Chen and Zahedi, 2016). Because this study is empirically tested based on experienced users in the US, the explanatory power could be limited when generalizing the study results to other populations with different user experiences and cultural backgrounds. Third, the contrast of cognitive and emotional mediators could lead to non-secure behavior in case emotion-focused logic dominates the appraisal process, according to EPPM. By theorizing the contrast between two indirect effects, researchers can make specific theoretical propositions, explanations, and even predictions about what behavioral outcomes can induce (e.g., dominated either by the fear control logic or the danger control logic) and further validate this issue based on different ISec contexts.

7. Conclusions

An important research domain in behavioral information security (ISec) is explaining or improving users' IS security behavior (intentions). For this purpose, many ISec scholars examining users' behavior (intention) have often applied health psychology theories, such as the extended parallel process model (EPPM). A fundamental theoretical assumption in EPPM (Witte, 1992, 1994; 1996) is dominant mediation, namely the assumption that individuals' behavior is driven by either danger control or fear control processes, is a fundamental theoretical assumption in EPPM (Witte, 1992, 1994; 1996). While dominant mediator assumption is an essential theoretical assumption of EPPM, the extant IS security research has largely ignored the value of testing and reporting dominant mediator assumption. In this paper, we reintroduce the theoretical origins of dominant mediator assumption and highlight the potential theoretical and practical merits by testing and reporting it in the context of anti-malware software use among experienced household users. We also argue that discriminant value equation introduced by Witte (1995), tested by Witte et al. (1996), and enhanced by Chen et al. (2021) is problematic. To this end, we proposes to assess the dominant mediator via a multiple mediation model instead of using the discriminant value equation.

CRediT authorship contribution statement

Yitian Xie: Conceptualization, Data curation, Formal analysis, Funding acquisition, Methodology, Writing – original draft, Writing – review & editing. **Mikko Siponen:** Conceptualization, Data curation, Funding acquisition, Investigation, Project administration, Supervision, Writing – original draft, Writing – review & editing. **Gabriella Laatikainen:** Methodology, Supervision, Validation, Writing – review & editing. **Gregory D. Moody:** . **Xiaosong Zheng:** Conceptualization, Data curation, Project administration, Resources, Software, Writing – review & editing.

Declaration of competing interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Data availability

Data will be made available on request.

Appendix 1. Survey

Survey

Instructions: This study aims to collect your opinions about the user experience of anti-malware applications in your home computer(s). We want you to pay careful attention to the survey and respond according to your real situation, please be assured that there are no wrong or right answers and that your responses will be kept confidential.

I have read and understood the above text.

I have installed an anti-malware application on my home computer(s). Yes / No

1. What is your age?
2. What is your gender? Male/Female
3. What is the highest level of education that you have completed?

1) High school 2) Vocational/Technology application college 3) Bachelor's degree 4) Master's degree 5) Doctorate/Ph. D. 6) Others

4. How many years have you been using computers?
5. How many years have you been using anti-malware software?

Please answer the following questions according to the following scale.

1=strongly disagree; 2=disagree; 3=somewhat disagree; 4=neither agree nor disagree; 5=somewhat agree; 6=agree; 7=strongly agree

Fear (Osman et al., 1994**))**

I feel anxious if malware infect my home computer(s).

(*continued on next page*)

(*continued*)

I feel afraid if malware infect my home computer(s).
I feel terrified if malware infect my home computer(s).
Instruction: Based on your past usage experience and general belief, you think:
Perceived Threat (Warkentin et al., 2016a**)**
VUL 1 Malware is a threat to my computer.
VUL 2 My computer is at risk of getting malware
VUL 3 Malware is a potential danger to my computer.
Instruction: Based on your past usage experience and general belief, you think:
Perceived Effectiveness (Warkentin et al., 2016a**)**
EFFICACY 1 Anti-malware applications work for computer protection.
EFFICACY 2 Anti-malware applications are effective for computer protection.
EFFICACY 3 When using an anti-malware application, a computer is more likely to be protected from malware.
Instruction: Based on your past usage experience, to what extend will you continue using anti-malware software on your home computer?
Continued Use Intention (Warkentin et al., 2016a**)**
CONT 1 I intend to run an anti-malware application on my home computer(s) in the next two weeks.
CONT 2 I am likely to run an anti-malware application on my home computer(s) in the next two weeks.
CONT 3 I plan to run an anti-malware application on my home computer(s) in the next two weeks.
Marker variable:
Masculinity/Femininity (Hofstede, 2001**)**
MAS1 Men usually solve problems with logical analysis; women usually solve problems with intuition.
MAS1 Solving problems usually requires an active forcible approach, which is typical of men.
MAS1 It is preferable to have a man in a high-level position rather than a woman.
Items to check the poor-quality responses
For this question only answer 5, somewhat disagree; do not give any other answer.
For this question only answer 2, agree; do not give any other answer.

Appendix 2. The Theoretical Origins of Multiple Mediation Assumption

The Mediation Relationship (IV-MEs-DV) in the Fear Appeal Theories

All these four theories (PMT, PMT2, PRM, and EPPM) highlight the multiple mediation assumptions of the fear appeal theories.[9] Specifically, they demonstrate the multiple mediation assumptions (IV-MEs-DV) as the source of information (IV), the cognitive appraisals (MEs), and the cognitive outcome (DV) (Leventhal, 1970, 1971; Rogers, 1975; Maddux and Rogers, 1983; Witte, 1992; 1994). The following table shows several seminal works in the fear appeal theories.

Theory	Source of Information (IV)	Cognitive Mediating Process (MEs)	Cognitive Outcome (DV)
The Parallel Response Model (Leventhal, 1970, 1971)	***External Danger* (external stimuli)** (e.g., message or actual danger). ***Internal Cues* (Internal reference)** 1) The person's emotional behavior. 2) The person's coping behavior.	The *Cognitive Encoder*. A ***parallel*** or sequential cognitive *mediation* process of danger control and fear control.	1) Danger control. 2) Fear response.
Original PMT (Rogers, 1975)	1) Magnitude of noxiousness. 2) Probability of occurrence. 3) Efficacy of recommended response.	1) Appraised severity. 2) Expectancy of exposure. 3) Belief in efficacy of coping response.	Intent to adopt recommended response.
Revised PMT (Maddux and Rogers, 1983)	***Environmental* (external stimuli)** • Verbal persuasion • Observational learning ***Intrapersonal* (Internal reference)** • Personality variables • Prior experience	*Threat Appraisal* • Intrinsic rewards • Extrinsic rewards • Severity • Vulnerability *Coping Appraisal* • Response efficacy • Self-efficacy • Response cost	Action or Inhibition of Action • Single act • Repeated acts • Multiple acts • Repeated multiple acts
Extended Parallel Process Model (Witte, 1992 1994)	***External Stimuli*** Message Components: • Self-efficacy • Response efficacy • Susceptibility • Severity ***Individual Difference* (Internal reference)**	1) Perceived Efficacy 2) Perceived Threat 3) Fear	1) Protection motivation (message acceptance). 2) Defensive motivation (message rejection).

[9] The multiple mediation assumptions in fear appeal theories include mediation assumptions, multiple mediation assumptions, and sequential mediation assumptions. Based on the range of this study, we focus on explaining the value of testing and reporting multiple mediation assumptions.

Appendix 3. The Theoretical and Statistical Meaning of Multiple Mediation (MEs)

We introduce that MMA, as a key theory assumption in fear appeal theories, can contribute to theory testing and theory contextualization for future study (Busse et al., 2017; Hong et al., 2014; Rucker et al., 2011; Zhao et al., 2010). There is a necessity to distinguish MMA as a theory assumption as well as a statistical method.

Appendix 3.1 The Statistical Meaning of Effect Size in Mediation Analysis

Terms	Definition	*Statistical meaning of mediation*	Mathematical expression
Mediation with one mediator			
Total effect	The sum of the direct and indirect effects.	The regression weight of the DV on the IV.	$c = ab + c'$
Direct effect	The direct effect of IV on DV	Identify whether the direct effect exist.	c'
Indirect effect	The product of the two unstandardized paths coefficient.	Identify whether the indirect effect exist.	ab
Mediation with multiple mediators			
Total effect	The sum of the direct and indirect effects.	The regression weight of the DV on the IV.	$c = ab + c'$ $c = a_1b_1 + a_2b_2 + c'$
Direct effect	The direct effect of IV on DV	Identify whether the direct effect exist.	c'
Total indirect effect	Testing the total indirect effect of IV on DV is analogous to conducting a regression analysis with several predictors.	1) To determine whether an overall indirect effect exists. 2) If an effect is found, one can conclude that the set of *j* variables mediates the effect of IV on DV.	$a_1b_1 + a_2\ b_2 + \ldots + a_j\ b_j$
Specific indirect effect	To determine to what extent specific *M* variables, mediate the IV-DV effect, conditional on the presence of other mediators in the model.	The specific indirect effect through M_j represents the ability of M_j to mediate the effect of IV on DV conditional on the inclusion of the other mediators in the model.	a_1b_1 a_2b_2
Contrast between two indirect effects (*contrast*)	To test if there is a significant difference of contribution to the DV between two mediators.	1) To determine the ***relative magnitudes*** of the specific indirect effects associated with all mediators. 2) Including two (or more) mediators in the same model is one way to pit competing theories against one another within a single model. 3) The quantification of indirect effects allows the investigator to answer such questions as whether the specific indirect effect of X on Y through proposed Mediator 1 differs in size from specific indirect effect through proposed Mediator 2.	$\mathbf{f}_c = a_1b_1 - a_2b_2.$ $\mathrm{var}[\mathbf{f}_c] = b_1^2\sigma_{a_1}^2 + b_2^2\sigma_{a_2}^2 + a_1^2\sigma_{b_1}^2$

Appendix 3.2 The Theoretical Meaning of Effect Sizes in Mediation Analysis

Terms	*Theoretical meaning of multiple mediation*	
Contrast between two indirect effects	To test if there is a significant difference between Mediator 1 and Mediator2 (e.g., Fear vs. Perceived Efficacy) can contribute to the DV (i.e., danger control process or emotion-focused coping response).	To test if the danger control process significantly differs from the fear control process. A coping response initiated by the danger control process will come when the danger control process mechanism surpasses the fear control process. In contrast, a coping response initiated by the fear control process will come when the fear control process surpasses the danger control process. **(Use *EPPM* (Witte, 1992, 1994) as an example)** To test if the perceived reward is significantly different from the perceived cost. An adaptive coping response will come when perceived reward surpasses perceived cost, while a maladaptive coping response will come when perceived cost surpasses perceived reward. **(Use *Revised PMT* (Maddux and Rogers, 1983) as an example)**

References

Angrist, J.D., Pischke, J.S., 2009. Mostly Harmless Econometrics: An Empiricist's Companion. Princeton university press.

Aurigemma, S., Mattson, T., 2018. Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. Comput. Secur. 73, 219–234. https://doi.org/10.1016/j.cose.2017.11.001.

Bhattacherjee, A., Lin, C.P., 2015. A unified model of IT continuance: three complementary perspectives and crossover effects. Eur. J. Inf. Syst. 24 (4), 364–373.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., 2015. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Q. 39 (4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5.

Bullock, J.G., Green, D.P., Ha, S.E., 2010. Yes, but what's the mechanism? (don't expect an easy answer). J. Pers. Soc. Psychol. 98 (4), 550.

Busse, C., Kach, A.P., Wagner, S.M., 2017. Boundary conditions: what they are, how to explore them, why we need them, and when to consider them. Organ Res Methods 20 (4), 574–609. https://doi.org/10.1177/1094428116641191.

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

Chen, Y., Zahedi, F.M., 2016. Individuals' internet security perceptions and behaviors. MIS Q. 40 (1), 205–222.

Davison, R.M., Martinsons, M.G., 2016. Context is king! Considering particularism in research design and reporting. J. Inf. Technol. 31 (3), 241–249.

Fairchild, A.J., MacKinnon, D.P., Taborga, M.P., Taylor, A.B., 2009. R 2 effect-size measures for mediation analysis. Behav. Res. Methods 41 (2), 486–498. https://doi.org/10.3758/BRM.41.2.486.

Fritz, M.S., MacKinnon, D.P., 2007. Required sample size to detect the mediated effect. Psychol. Sci. 18 (3), 233–239. https://doi.org/10.1111/j.1467-9280.2007.01882.x.

Gefen, D., Rigdon, E.E., Straub, D., 2011. Editor's comments: an update and extension to SEM guidelines for administrative and social science research. MIS Q. iii-xiv.

Hayes, A.F., 2009. Beyond baron and kenny: statistical mediation analysis in the new millennium. Commun. Monogr. 76 (4), 408–420. https://doi.org/10.1080/03637750903310360.

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

Hofstede, G., 2001. Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations. Sage.

Hong, W., Chan, F.K.Y., Thong, J.Y.L., Chasalow, L.C., Dhillon, G., 2014. A framework and guidelines for context-specific theorizing in information systems research. Inf. Syst. Res. 25 (1), 111–136. https://doi.org/10.1287/isre.2013.0501.

Imai, K., Keele, L., Tingley, D., Yamamoto, T., 2011. Unpacking the black box of causality: learning about causal mechanisms from experimental and observational studies. Am. Polit. Sci. Rev. 105 (4), 765–789.
Jackson, D.L., 2003. Revisiting sample size and number of parameter estimates: some support for the N:q hypothesis. Struct. Eq. Model.: Multidiscip. J. 10 (1), 128–141. https://doi.org/10.1207/S15328007SEM1001_6.
Johnston & Warkentin, 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 549. https://doi.org/10.2307/25750691.
Johnston, A.C., Warkentin, M., Siponen, M., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. 39 (1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06.
Kelly, S., 2010. Qualitative interviewing techniques and styles. In: Bourgeault, I, Dingwall, R, de Vries, R (Eds.), The Sage Handbook of Qualitative Methods in Health Research. Sage Publications, Thousand Oaks.
Kline, R.B., 2023. Principles and Practice of Structural Equation Modeling, 5thed. Guilford publications.
Leventhal, H., 1970. Findings and theory in the study of fear communications. In: Advances in Experimental Social Psychology, 5. Elsevier, pp. 119–186. https://doi.org/10.1016/S0065-2601(08)60091-X.
Leventhal, H., 1971. Fear appeals and persuasion: the differentiation of a motivational construct. Am. J. Public Health 61 (6), 1208–1224.
Liang, H., Xue, Y., Pinsonneault, A., Wu, Y.A., 2019. What users do besides problem-focused coping when facing IT security threats: an emotion-focused coping perspective. MIS Q. 43 (2), 373–394.
Lowry, P.B., Moody, G.D., Parameswaran, S., Brown, N., 2023. Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. J. Manag. Inf. Syst. https://doi.org/10.2139/ssrn.4416590.
Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19 (5), 469–479.
Martens, M., De Wolf, R., De Marez, L., 2019. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Comput. Human. Behav. 92, 139–150. https://doi.org/10.1016/j.chb.2018.11.002.
Moody, G.D., Siponen, M., Pahnila, S., 2018. Toward a unified model of information security policy compliance. MIS Q. 42 (1), 285–311. https://doi.org/10.25300/MISQ/2018/13853.
Ortiz de Guina, A., Markus, M.L., 2009. Why break the habit of a lifetime? Rethinking the roles intention, habit, and emotion in continuing information technology use. MIS Q. 33, 433–444.
Osman, A., Barrios, F.X., Osman, J.R., Schneekloth, R., Troutman, J.A., 1994. The Pain Anxiety Symptoms Scale: psychometric properties in a community sample. J. Behav. Med. 17, 511–522.
Podsakoff, P.M., MacKenzie, S.B., Podsakoff, N.P., 2012. Sources of method bias in social science research and recommendations on how to control it. Annu. Rev. Psychol. 63 (1), 539–569. https://doi.org/10.1146/annurev-psych-120710-100452.
Pirlott, A.G., MacKinnon, D.P., 2016. Design approaches to experimental mediation. J. Exp. Soc. Psychol. 66, 29–38.
Posey, C., Bennett, R.J., Roberts, T.L., 2011. Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. Comput. Secur. 30 (6–7), 486–497.
Preacher, K.J., Hayes, A.F., 2008. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behav. Res. Methods 40 (3), 879–891. https://doi.org/10.3758/BRM.40.3.879.
Robinson, O.C., 2014. Sampling in interview-based qualitative research: a theoretical and practical guide. Qual. Res. Psychol. 11 (1), 25–41.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. J. Psychol. 91 (1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.
Rucker, D.D., Preacher, K.J., Tormala, Z.L., Petty, R.E., 2011. Mediation analysis in social psychology: Current practices and new recommendations. Soc. Pers. Psychol. Compass 5 (6), 359–371.
Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behaviour formation in organizations. Comput. Secur. 53, 65–78.
Shrout, P.E., Bolger, N., 2002. Mediation in experimental and nonexperimental studies: new procedures and recommendations. Psychol. Methods 7 (4), 422.
Siponen, M., Rönkkö, M., Fufan, L., Haag, S., Laatikainen, G., 2023. Protection Motivation Theory in information security behavior research: reconsidering the fundamentals. Commun. Assoc. Inf. Syst. 53. https://aisel.aisnet.org/cais/vol53/iss1/47.
Vedadi, Ali, Warkentin, M., 2018. Secure Behavior over time: perspectives from the theory of process memory. ACM SIGMIS Database: Database Adv. Inf. Syst. 49, 39–48. https://doi.org/10.1145/3210530.3210534.
Vedadi, A., Warkentin, M., 2020. Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. J. Assoc. Inf. Syst. 21 (2), 3. https://aisel.aisnet.org/jais/vol21/iss2/3.
Warkentin, M., Johnston, A.C., Shropshire, J., Barnett, W.D., 2016a. Continuance of protective security behavior: a longitudinal study. Decis. Support Syst. 92, 25–35. https://doi.org/10.1016/j.dss.2016.09.013.
Warkentin, M., Walden, E., Johnston, A., Straub, D., 2016b. Neural correlates of protection motivation for secure IT behaviors: an fMRI examination. J. Assoc. Inf. Syst. 17 (3), 194–215. https://doi.org/10.17705/1jais.00424.
Witte, K., 1992. Putting the fear back into fear appeals: the extended parallel process model. Commun. Monogr. 59 (4), 329–349. https://doi.org/10.1080/03637759209376276.
Witte, K., 1994. Fear control and danger control: a test of the extended parallel process model (EPPM). Commun. Monogr. 61 (2), 113–134. https://doi.org/10.1080/03637759409376328.
Witte, K., 1995. Generating effective risk messages: how scary should your risk communication be? Annal. Int. Commun. Assoc. 18 (1), 229–254. https://doi.org/10.1080/23808985.1995.11678914.
Witte, K, 1996. Fear as motivator, fear as inhibitor: using the extended parallel process model to explain fear appeal successes and failures. In: Andersen, P.A., Guerrero, L. K. (Eds.), Handbook of Communication and Emotion: Research, Theory, Applications, and Contexts. Academic Press, pp. 423–450.
Witte, K., Cameron, K.A., McKeon, J.K., Berkowitz, J.M., 1996. Predicting risk behaviors: development and validation of a diagnostic scale. J. Health Commun. 1 (4), 317–341. https://doi.org/10.1080/108107396127988.
Xie, Y., Siponen, M., Moody, G., Zheng, X., 2022. Discovering the interplay between defensive avoidance and continued use intention of anti-malware software among experienced home users: a moderated mediation model. Inf. Manag. 59 (2), 103586 https://doi.org/10.1016/j.im.2021.103586.
Zhao, X., Lynch, J.G., Chen, Q., 2010. Reconsidering baron and kenny: myths and truths about mediation analysis. J. Consum. Res. 37 (2), 197–206. https://doi.org/10.1086/651257.

Yitian Xie is an Assistant Professor in the Intelligent Operations and Marketing Department at Xi'an-Jiaotong Liverpool University. She received her doctoral degree in Information Systems from the University of Jyväskylä, Finland. Her research interests lie in behavioral information security, information security awareness, education & training, and e-business strategy & analytics. Her work has been published in *Information & Management* and *European Journal of Information Systems*.

Mikko Siponen is a Professor of Information Systems at the University of Alabama. He has a Ph.D. in Philosophy and a Ph.D. in Information Systems. He is an invited member of the Finnish Academy of Science and Letters. He has worked in several countries as a visiting professor, honorary professor, invited speaker, and a consultant. He has been Primary Investigator for research projects funded by the Academy of Finland, the EU, Business Finland.

Gabriella Laatikainen is a Senior Scientist at VTT Technical Research Centre of Finland. She pursued her Ph.D. in Economics and Business Administration (Information Systems) at the University of Jyväskylä. Her current research interests lie in business aspects and governance of ecosystems that are built around emerging technologies, such as self-sovereign identity, blockchain, and cloud computing. Her work has been published in *Decision Support Systems, Journal of Systems and Software, and Information and Software Technology*.

Greg Moody is an Associate Professor of Information Systems and Graduate Director at the University of Nevada, Las Vegas (UNLV). He serves as Director of the M.S. Management Information Systems, the M.S. Data Analytics, and Applied Economics, and the Data Analytics Certificate programs. He also holds a Lee Professorship within the Lee Business School. His-work has appeared in various journal outlets, including the most prestigious journals in his field: *Information Systems Research, Management Information Systems Quarterly, Criminology*, and *Justice Quarterly*. Most of this work has been focused on identifying managerial methods to encourage compliance with security policies to increase the security postures of organizations.

Xiaosong Zheng is a professor in Business Administration at Shanghai University, China, and Tallinn University of Technology, Estonia. He received a Ph.D. in IT from the University of Oulu in 2007. He also holds an MSc in Accounting from the University of Oulu and an MSc in Economics from Hanken School of Economics. He has published widely in the business and IT fields.