JYU DISSERTATIONS 772

Tong Xin

Securing the Human Factor

Understanding the Role of Prior Experience, Mental Representations, and Coping Strategies in Behavioral Information Security

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 772

Tong Xin

Securing the Human Factor

Understanding the Role of Prior Experience, Mental Representations, and Coping Strategies in Behavioral Information Security

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi Agoran auditoriossa 2
huhtikuun 27.päivänä 2024 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on April 27, 2024, at 12 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2024

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Päivi Vuorio
Open Science Centre, University of Jyväskylä

ISBN 978-952-86-0122-7 (PDF)
URN:ISBN:978-952-86-0122-7
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-952-86-0122-7

ABSTRACT

Xin, Tong
Securing the Human Factor: Understanding the Role of Prior Experience, Mental Representations, and Coping Strategies in Behavioral Information Security
Jyväskylä: University of Jyväskylä, 2024, 90 p.
(JYU Dissertations
ISSN 2489-9003; 772)
ISBN 978-952-86-0122-7 (PDF)

Although Protection Motivation Theory (PMT), originally from health psychology, has become a foundational theory for explaining information security (ISec) related behaviors, it has not been fully applied to ISec. This is because several core components of PMT are completely ignored, such as users' ISec-related prior experiences and coping styles. To rectify this, this dissertation consists of three studies exploring individual users' prior ISec experiences, their cognitive processing of fear appeal messages, and emotion-focused coping (EFC) strategies in coping with ISec threats.

In Study 1, we expand on the commonly simplified notion of Prior Experience (PE) in ISec, accentuating the influence of both direct and vicarious experiences. Emphasizing the importance of prior coping feedback, the research unpacks how threat and coping appraisals mediate the effects of prior experiences on present protective intentions related to cybersecurity, while also shedding light on potential cognitive biases. In turn, Study 2 delves into the realm of fear appeal messages, using Construal Level Theory (CLT) to highlight the pivotal role of individual users' mental representations in decoding these messages. Experimental outcomes confirm the significant impact of specific mental representations on user responses, suggesting novel pathways to refine ISec communication strategies. Lastly, a subtle exploration of emotion-focused coping (EFC) within ISec is undertaken in Study 3. Going beyond the commonly studied problem-focused coping, this segment discerns active and passive inward EFC strategies, revealing their inherent complexities and implications on perceived threat vulnerability.

This dissertation enhances the application of PMT in the field of information security. By conducting an in-depth exploration of the previously overlooked components of PMT, this dissertation offers an enriched perspective for understanding individual user ISec behaviors, which provides researchers with a more sophisticated and comprehensive approach to interpreting user behavior in ISec contexts. The investigations in three studies furnish crucial insights for the enhancement of both ISec research methodologies and practical cybersecurity measures.

Keywords: behavioral information security, Protection Motivation Theory (PMT), prior experience, mental representation, inward emotion-focused coping

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Xin, Tong
Ihmistekijän turvaaminen: Ymmärrys aikaisemmasta kokemuksesta, mentaalisista representaatioista ja selviytymisstrategioista käyttäytymistiedotusturvallisuudessa
Jyväskylä: Jyväskylän yliopisto, 2024, 90 s.
(JYU Dissertations
ISSN 2489-9003; 772)
ISBN 978-952-86-0122-7 (PDF)

Vaikka alun perin terveyspsykologiasta peräisin oleva suojamotivaatioteoria on muodostunut keskeiseksi teoriaksi selittämään tietoturvakäyttäytymistä, teorian alan sovelluksissa on muutamia puutteita. Tämä johtuu siitä, että useita teorian keskeisiä komponentteja on sivuutettu, kuten käyttäjien aiemmat tietoturvakokemukset ja selviytymistyylit. Tämän problematiikan korjaamiseksi tämä väitöskirja koostuu kolmesta tutkimuksesta, jotka tarkastelevat yksittäisten käyttäjien aiempia tietoturvakäyttäytymiseen liittyviä kokemuksia, heidän kognitiivista prosessointiaan pelotteluviestejä saatuaan ja tunnekeskeisiä selviytymisstrategioita vastauksena uhkiin.

Tutkimuksessa 1 laajennamme yleisesti yksinkertaistettua käsitystä aikaisemmasta tietoturvakokemuksesta korostaen sekä suorien että välillisten kokemusten vaikutusta. Aiemman selviytymispalautteen tärkeyttä painottaen tutkimus selittää, miten uhka- ja selviytymisarviot välittävät aikaisempien kokemusten vaikutuksia nykyisiin suojautumisaikomuksiin samalla, kun se tuo uutta näkemystä mahdollisiin kognitiivisiin vinoumiin. Tutkimus 2 liittyy pelkoon vetoaviin viesteihin. Konstruktiotason teoriaa käyttäen tarkastellaan yksittäisten käyttäjien mentaalisten representaatioiden keskeistä roolia tällaisten viestien tulkitsemisessa. Kokeelliset tulokset osoittavat tiettyjen mentaalisten representaatioiden vaikuttavan merkittävästi käyttäjävasteisiin ja tuovat esiin uusia keinoja parantaa kyberturvallisuuden viestintästrategioita. Lopuksi tutkimus 3 käsittelee yksityiskohtaisesti emotionaalisiin strategioihin keskittyvää selviytymistä kyberturvallisuudessa. Lisänä yleisesti tutkittuun ongelmalähtöiseen selviytymiseen tämä tutkimus erittelee aktiivisia ja passiivisia sisäisiä selviytymisstrategioita paljastaen niiden luontaisen monimutkaisuuden ja vaikutuksen koettuun uhkahaavoittuvuuteen.

Tämä väitöskirja laajentaa suojamotivaatioteorian soveltamista tietoturvan alalla. Nämä tutkimukset tarjoavat tutkijoille kehittyneemmän ja kattavamman lähestymistavan käyttäjien käyttäytymisen tulkintaan tietoturvakontekstissa.

Avainsanat: kyberturvakäyttäytyminen, suojamotivaatioteoria, aikaisempi kokemus, mentaalinen representaatio, sisäänpäin suuntautunut emotionaalinen selviytymiskeino

Author

Tong Xin
Faculty of Information Technology
University of Jyväskylä
Finland
toxin891125@gmail.com
orcid.org/0000-0002-9016-9680

Supervisors

Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers

Karen Renaud
Faculty of Computer and Information Sciences
University of Strathclyde
UK

Xin (Robert) Luo
Robert O. Anderson School of Management
University of New Mexico
USA

Opponent

Huigang Liang
Department of Management Information Systems
Fogelman College
University of Memphis
USA

ACKNOWLEDGEMENTS

Embarking on a PhD journey is like being on a long journey of knowledge discovery and self-discovery. This journey, filled with doubt, excitement, and profound learning, would have been impossible without the support of many incredible individuals. With deep gratitude, I would like to express my heartfelt thanks to those who assisted me in completing my doctoral research.

First, I sincerely thank my supervisor, Mikko Siponen, whom I admire and feel incredibly fortunate to have met and had the opportunity to learn from. He led me on my academic journey and thus positively impacted my lifestyle. The guidance he provided during my exploration of doctoral research topics allowed me to successfully find the research direction that interests me. His comments and feedback on my thesis honed my ability to think and write with greater rigor and scientific precision. He encouraged me to think critically and independently, which not only helped my academic literacy but also allowed me to interpret daily matters from more perspectives. I also benefited a lot from his critical thinking and unique insights in teaching. Most importantly, it was his introduction to floorball that turned it into my favorite sport and hobby. I am proud that he is my supervisor throughout my long doctoral journey.

In the process of thesis publication and doctoral graduation, I sincerely thank my reviewers, Dr. Karen Renaud, Professor Xin (Robert) Luo, whose insightful and friendly comments gave me the opportunity to enhance the quality of my thesis and consider future research directions. I am deeply grateful to Prof. Huigang Liang for accepting the role of my opponent amidst his busy schedule and dedicating himself to examining my work. Furthermore, I would like to thank my colleagues from the PhD graduation team, Marja-Leena Rantalainen, Nina Pekkala, Heikki Karjaluoto, for their seamless coordination and assistance with the publication of the thesis.

I would like to extend my special thanks to my colleagues for any help they provided me during my doctoral studies. Thanks to Mikko Rönkkö for spending a substantial amount of time helping me learn quantitative analysis and survey development methods. Thanks to Fufan Liu, Yitian Xie, Naomi Woods, Jing Liu, Hanna Paananen and Piia Perälä for sharing their research experiences with me. Thanks to Tapio Tammi for organizing the weekly floorball activities. Thanks to Ying Li for having me as a collaborator on her research project.

To my dear friends, both near and far, who have provided endless encouragement, laughter, and a listening ear during moments of stress and success, I am forever grateful.

Finally, I would like to express my warmest thanks to my family. Their love and sacrifice laid the foundation for me, and words cannot express how grateful I am. The gratitude I hold for my mother, with her unconditional love, patience, and companionship, has given me the strength to continue this challenging yet meaningful path. I am sincerely thankful to my partner, whose comfort and humorous yet wise view of life helped me through the most difficult psychological times. Thanks to my partner's loving family for their unwavering

help and support, providing me with countless joyful moments and warm, loving memories. Thanks to my little one, who has allowed me to see the world in a different light. Your trust in me is like the wind under my wings, pushing me forward through adversity.

As I reflect on this journey, I realize that this achievement is not solely mine but a culmination of the contributions, support, and faith of all the individuals mentioned above. To everyone who has been a part of my PhD journey, whether named or appreciated in silence, thank you for playing a role in shaping my research and my path as a scholar.

Jyväskylä 3.4.2024
Tong Xin

FIGURES

TABLES

ABBREVIATIONS

ANOVA	Analysis of Variance
AVE	Average Variance Extracted
CLT	Construal Level Theory
EFC	Emotion-focused Coping
EPPM	Extended Parallel Process Model
ISec	Information Security
MANCOVA	Multivariate Analysis of Covariance
MDT	Moral Disengagement Theory
MIS	Management Information Systems
OS	Operating System
PDE	Prior Direct Experience
PE	Prior Experience
PFC	Problem-focused Coping
PMT	Protection Motivation Theory
PVE	Prior Vicarious Experience
SEM	Structural Equation Modelling
SETA	Security Education, Training, and Awareness
TTAT	Technology Threat Avoidance Theory

CONTENTS

1 INTRODUCTION

The proliferation of mobile devices and the exponential growth of mobile applications cater to the needs of users to perform various tasks including banking, shopping, communication, and entertainment. Mobile devices are increasingly becoming more ubiquitous than desktops and laptops, making them prime targets for cyber threats, especially mobile malware (“2023 Data Breach Investigations Report,” 2023). Mobile malware has evolved rapidly, with various types such as trojans, spyware, ransomware, and adware specifically targeting mobile platforms (“Global Mobile Threat Report 2023,” 2023). While technology countermeasures are essential, the significance of human factors in security breaches of mobile devices, stemming from actions such neglecting system update neglect and the reuse of weak password, is undeniable (Johnston et al., 2015; Li et al., 2019; Moody et al., 2018). Given that human behaviors often contribute substantially to ISec incidents, management information systems (MIS) research emphasizes understanding these behaviors and crafting behavioral interventions, thereby enhancing security in both public and private spheres (Boss et al., 2015; Y. Chen & Zahedi, 2016; Li et al., 2022; Woods & Siponen, 2019). Such cybersecurity behaviors are studied under different names, including awareness (M. T. Siponen, 2000), computer abuse and misuse (Goodhue & Straub, 1991) , risky behavior, ISec policy violations and ISec policy compliance.

The behavioral information security branch of the field of information systems, given its nascent status within the social sciences, has been significantly influenced by theories from as diverse disciplines as ethics (M. Siponen, 2001), moral psychology, health psychology (Boss et al., 2015; Johnston et al., 2015), criminology (Goodhue & Straub, 1991), and others (Moody et al., 2018). A notable exemplar is the Protection Motivation Theory (PMT) by Rogers (1975, 1983), initially rooted in health psychology (M. Siponen et al., 2023). Over time, PMT has become among one of the most well-known model for explaining ISec behavior (Boss et al., 2015). However, the current application of PMT in information security often focuses narrowly on aspects such as cognitive factors and fear appeals, overshadowing other components Rogers originally proposed (Haag et al., 2021). Some ISec studies, even those purporting to explore PMT's "full nomology", have overlooked certain elements (Boss et al., 2015), potentially limiting the theory's comprehensive utility (see also Siponen et al., 2023).

The scientific background of this dissertation is motivated by these concerns through three empirical studies, focusing on individual users' ISec related prior experience, their mental representation of fear appeal messages, and their emotion-focused coping (EFC) strategies to ISec threats. Utilizing survey-based cross-sectional studies and quantitative methodologies, this work assesses the influence of these elements on individual ISec protective behaviors. The aim of this dissertation is to illuminate neglected behavioral drivers in PMT, offer deeper insights, and provide a comprehensive understanding of individual choices regarding ISec behaviors.

Study 1 explored the impact of individual users' ISec related prior experience on their protection intentions. It provides a perspective to help understand individuals' preferences for evaluating fear appeal messages (Study 2) and adopting coping strategies related to ISec threats (Study 3). For example, negative feedback on previous coping behaviors may promote individuals' inward emotion-focused coping strategies. Study 2 further explored how individual users decode fear appeal messages by highlighting the critical role of their mental representations. This is a key link in understanding how users form protective intentions, and is crucial to understanding how individuals made their choice of coping strategies based on cognition in Study 3. The experimental results confirmed the significant impact of specific mental representations on user responses and proposed new ways to improve ISec communication strategies. Study 3 explored how the cognitive evaluation process of ISec threats affects individuals' use of inward emotion-focused coping strategies. This is another important link in understanding user protective behavior in ISec, because the choice of coping strategies will directly affect the users' protective behavior. This study goes beyond commonly studied problem-focused coping to reveal active and passive inward emotion-focused coping strategies. Collectively, these three studies together form a complete framework for understanding how users evaluate ISec threats, form protective intentions, and choose coping strategies. This framework not only helps us better understand users' ISec behaviors, but also provides guidance for designing effective ISec interventions.

The research questions, methods, and main contributions of the three studies are summarized in Table 1.

TABLE 1 The research questions, research methods and contributions of the dissertation

Studies	Research Question	Main Methods	Contribution
Study 1	How do prior experiences influence individuals' cognitive and behavioral patterns in information security?	Survey-based & quantitative analysis includes Structural Equation Modelling (SEM), chain mediation and moderation analysis	The study deepens the understanding of prior experience in information security, systematically examining its influence on individuals' ISec related cognitions and behavioral intentions.
Study 2	How can one leverage an individual's mental representation of fear appeal messages to enhance their persuasive efficacy?	Experiment & quantitative analysis includes SEM, mediation analysis	The study integrates construct level theory to delineate the characteristics of individuals' mental representation of fear appeal messages. Empirical evidence further demonstrates that manipulating mental representations enhances the persuasive efficacy of such messages.
Study 3	How do different inward emotion-focused coping strategies affect individual users' ISec behaviours?	Survey-based & quantitative analysis includes SEM	The study addresses the limited understanding and potential misconceptions of emotion-focused coping in the ISec literature by differentiating five inward EFC strategies and empirically exploring their effects on individuals' behavioral intentions.

Because all the results of the study are derived from data collected from participants, we make an ethical statement here. Throughout this thesis, we have adhered to the highest ethical standards to ensure the integrity, responsibility, and ethical treatment of all participants and data. This thesis has secured informed consent, confidentiality, and anonymity for all participants. The data collection and analysis procedures were designed to respect participants' rights and welfare, minimizing potential risks. Personal information has been de-identified and securely stored, accessible only to the research team, to protect participant privacy.

Since this dissertation mainly takes PMT as the theoretical background, Chapter 2 will briefly introduce PMT and its application and challenges in MIS field. Chapter 3 investigates the complex role of previous experiences in shaping how users approach information security. In Chapter 4, we study how ISec related fear-based messages are interpreted by users by applying CLT. Chapter 5 focuses on the inward EFC strategies individuals use to cope with ISec threats. In Chapter 6, we culminate in a comprehensive summary. The whole research is under the mobile malware context.

2 PMT AND ITS APPLICATIONS IN BEHAVIORAL INFORMATION SECURITY

In this Chapter, we will mainly review the theoretical background of PMT and its applications and challenges in the behavioral information security research field.

2.1 Theoretical background

In 1975, R.W. Rogers introduced the Protection Motivation Theory (PMT) to explain the influence of fear appeals—communications emphasizing potential adverse outcomes—on attitude and behavioral shifts. PMT emerges from the foundational research on fear control within the Parallel Process Model (PPM) (Leventhal, 1970). It integrates the concept of danger-control response from PPM, and further elaborates on strategies to augment individuals' capacity to effectively respond to perceived threats (Rogers, 1975). Originally, PMT aimed to comprehend the motivation behind actions taken in response to fear-inducing health threat communications. By 1983, Rogers had refined PMT, broadening its scope with additional elements (please see Figure 1 for the PMT framework).

PMT posits that various information sources, both environmental and intrapersonal, can trigger cognitive appraisals, subsequently influencing individuals’ intentions or behaviors (Floyd et al., 2000; Rogers et al., 1997). Environmental sources primarily encompass verbal persuasion, notably fear appeals, and observational learning. Fear appeals aim to incite fear and prompt specific actions by highlighting potential risks (Milne et al., 2000; Rogers, 1983), while observational learning derives from witnessing others' experiences (Rogers et al., 1997). Intrapersonal sources include individual personality traits and past experiences. Central to PMT are two cognitive appraisal processes that mediate the impact of threatening information on coping strategies (Rogers, 1983). The threat appraisal assesses perceived likelihood of personally experiencing the threat (threat vulnerability) and seriousness of the potential harm (threat severity). The greater the perceived threat to an individual, the more fear is aroused. Fear is considered an intervention variable in PMT, playing only an indirect role, measuring the degree of fear that an assessed threat induces in an individual (Milne et al., 2000; Rogers, 1983; Rogers et al., 1997).

While the coping appraisal evaluates the perceived effectiveness of the recommended response (response efficacy) and the belief in one's capability to execute that response (self-efficacy). This dual appraisal ultimately gives rise to the inclination to adhere to recommended protective measures, termed as 'protection motivation' (Rogers, 1983). Protection motivation is a positive linear function of the beliefs that (a) the threat possesses significant severity, (b) individuals are personally susceptible to said threat, (c) the suggested countermeasure is efficacious, and (d) individuals possess the capability to execute the recommended response. The cognitive appraisal process can also lead to maladaptive coping responses such as denial or avoidance. A maladaptive coping response is characterized by activities that primarily modulate the emotions invoked by a threat, instead of addressing the threat directly (Rogers et al., 1997). Studies have shown that while threat appraisal shares a positive correlation with maladaptive coping responses, coping appraisal conversely demonstrates a negative correlation with maladaptive coping responses (Floyd et al., 2000; Milne et al., 2000).

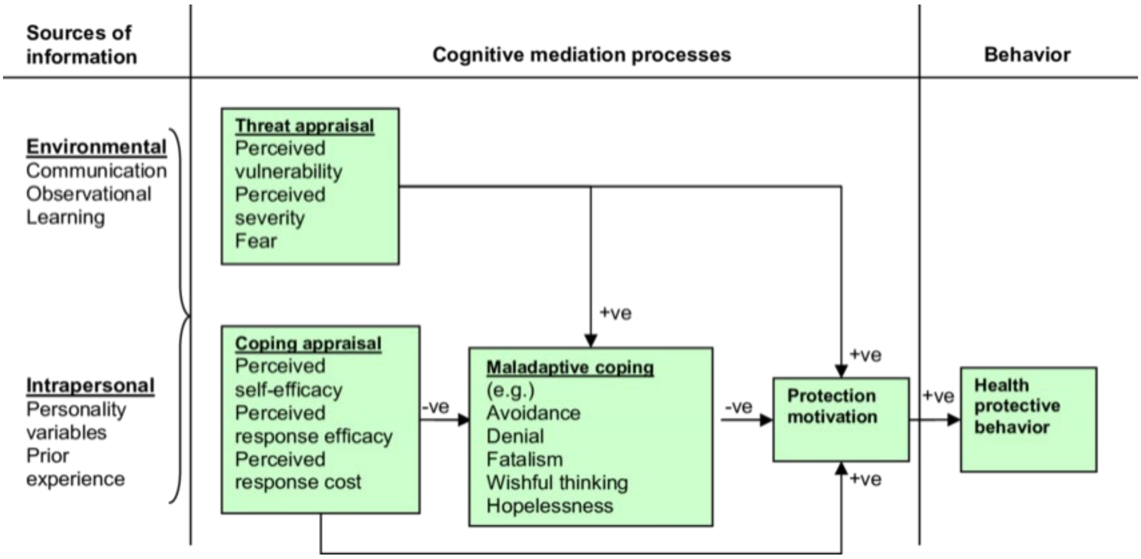


FIGURE 1 Protection motivation theory from Milne et al. (2000)

2.2 PMT in prior ISec research

In the realm of ISec research, PMT is employed by scholars to comprehend threat response intentions or to illustrate responses to fear appeal stimuli (Moody et al., 2018; Orazi et al., 2019). Among them, understanding users' ISec behavior is the most important application direction of PMT. From its initial applications in studies like Siponen et al.'s (2007) exploration of workplace ISec policy compliance, PMT has extensively informed research across diverse ISec behaviors and settings, encompassing from areas such as individual users' malware threat response and software utilization (Lee et al., 2008; Tsai et al., 2016), to organizational practices like ISec policy compliance and BYOD security (R. E. Crossler et al., 2014; Luuk et al., 2023; Vance et al., 2012). In these studies, most research models examine other behavioral constructs or theories together with PMT, such as deterrence theory (Herath & Rao, 2009; Pham et al., 2017; M. Siponen & Vance, 2010), theory of planned behavior (e.g., Bélanger et al., 2017; Ifinedo, 2012), technology acceptance model (Foth et al., 2012; Herath et al., 2014). This type of research predominantly utilized empirical cross-sectional methodologies, employing survey instruments to assess the variables influencing individuals' ISec behaviors. The findings offer strategic insights for corporations, institutions, and individuals aiming to enhance safe ISec practices. Several studies believe that the core of PMT lies in leveraging communicative strategies, notably fear appeals, to motivate users towards actions that safeguard information security (Boss et al., 2015). These investigations predominantly employ experimental research methodologies, focusing on the design and manipulation of fear appeal messages to glean insights into the execution of effective fear appeals in this context (e.g., Boss et al., 2015; Johnston et al., 2019; Orazi et al., 2019; Wall & Warkentin, 2019). In addition, PMT has also been widely used in some other directions, such as designing and evaluating ISec training programs. By understanding how individuals protect themselves from ISec threats, training can be tailored to increase the severity and sensitivity to these threats while providing effective response strategies, thus aiding in the development of effective training materials. When developing security technology, PMT can guide the design process to ensure solutions are user-friendly. Understanding the motivational factors that drive the use of security technologies could also help increase user acceptance and adoption of technology.

While PMT is being continuously integrated into the ISec research field, some challenges have also emerged. We will not go through all the challenges here; rather, we will highlight key ones. One challenge that is often mentioned is the conflicting empirical evidence for the conclusions of different PMT based ISec studies. For example, the role of threat and coping appraisals in predicting protective behavior exhibits mixed results. While studies such as Boss et al. (Boss et al., 2015) and Chen & Zahedi (2016) found a significant predictive role of threat appraisal in protective behaviors, other research, including Johnston et al. (2015), Crossler (2014), and Ng et al. (2009), failed to establish a positive correlation between perceived threats and protective intentions. Verkijika (2018) observed that the relevance of coping appraisal with protective intention appears to be marginal. In contrast, other empirical and meta-analytic data in ISec studies suggest a more substantial impact of coping appraisal variables within the PMT model on protection motivation (Mou et al., 2022). There have been some recent studies trying to explain or solve this issue from different perspectives. For instance, Ng et al. (2021) employed attitudinal ambivalence theory to account for inconsistent findings in PMT research. Mou et al. (2022) conducted a meta-analysis of 92 PMT-based studies, assessing the interrelationships among PMT constructs. The views put forward by Aurigemma & Mattson (2019) and Siponen et al. (2023) also provide some important inspiration. Aurigemma & Mattson (2019) critiqued the generalizability of models for ISP compliance. As the security actions required for different ISec threats vary greatly, if one wants to improve the practical effect of the theory, one should consider that the specific context, and security actions for different threats may require different explanatory models. Siponen et al. (2023) further posited that contextualizing research, thereby narrowing its scope, is advantageous when it leads to improved explanatory or predictive precision, and explained the reasons for this point of view. From their point of view (Aurigemma & Mattson, 2019; M. Siponen et al., 2023), the inconsistencies in PMT-related ISec research findings may be caused by different study contexts, such as the nature of the subjects (individuals vs. organizational employees), types of threats, and cultural or environmental differences.

Moreover, a significant portion of the PMT-informed ISec research predominantly concentrates on threat and coping appraisals, thereby overlooking other critical components of PMT. As defined by Rogers et al. (1997), PMT is comprised of three principal elements: the source of information, the cognitive mediating process, and coping modes. An extensive review by Haag et al. (2021) of 67 PMT studies in the ISec domain revealed a pronounced focus on the cognitive mediating process. Predominantly researched PMT components include self-efficacy (91.0%), threat severity (89.6%), threat vulnerability (88.1%), response efficacy (83.6%), and protection motivation (71.6%) are the most common PMT components. Conversely, there is a noticeable dearth of research addressing other facets, such as personality variables and maladaptive coping strategies. Even studies by researchers such as Boss et al. (2015), which purport to encompass a 'full PMT nomology', tend to omit elements such as the source of information and coping modes (Siponen et al., 2023). We are not saying that “full nomology” must be used with every PMT application, because the issue of which constructs apply depends on the research goal or phenomenon of interest (Siponen et al., 2023). However, an excessive focus on cognitive mediation processes could potentially lead to an overemphasis on rational decision-making frameworks, thereby neglecting crucial emotional, psychological, and situational factors that significantly impact security behavior. This oversight in acknowledging components integral to PMT not only undermines the original intent of utilizing PMT to comprehend and elucidate user ISec behavior, but also risks a partial understanding of the processes involved. For instance, a lack of research on sources of information may lead to an incomplete understanding of threat appraisal. Similarly, examining a singular coping pattern, while disregarding alternative strategies, might yield a limited perspective on how individuals actually respond to ISec threats, failing to capture the full range of factors that dictate engagement in recommended security practices.

The personal relevance of ISec threats also poses challenge for PMT to further adapt to the ISec context. PMT was originally used in the healthcare field. Threats in this area are often directly related to an individual's health and well-being. The consequences of not following recommended behaviors (such as not exercising or eating unhealthy foods) can result in direct physical harm. It makes the threat very tangible and personal, which can motivate individuals to take protective action. In the ISec field, threats are often related to personal information or data. While these threats may have serious consequences (such as identity theft or financial loss), they may not be considered a direct hazard to an individual. It may make the threat appear less direct or personal, which may affect an individual's protective motivation.

To summarize, while the implementation of PMT in the ISec realm introduces certain challenges to its application, it does not detract from the theory's inherent value to the ISec. PMT continues to offer substantial insights into the comprehension and influence of individual ISec behaviors. This dissertation, set against the backdrop of mobile malware, endeavors to alleviate some of these challenges. It does so by executing three quantitative studies. According to PMT, in this dissertation, "perceived threat severity" is conceptualized as an individual's assessment of the potential adverse consequences of mobile malware attacks. "Perceived threat vulnerability" refers to one's estimation of the likelihood of encountering such a threat. "Perceived response efficacy" designates the belief that recommended preventive actions will effectively secure the mobile device, while "self-efficacy" pertains to one's confidence in executing these actions. "Protection intention" is operationalized as the proactive intent to update the mobile operating system promptly.

3 STUDY 1: EXPERIENCE MATTERS: INVESTIGATING THE ROLE OF PRIOR EXPERIENCE IN INFORMATION SECURITY PERFORMANCE

Prior experience (PE) is a substantial determinant of ISec intentions and actions, particularly among users with limited ISec training. Yet, this pivotal aspect is often simplified in ISec research, being reduced to prior exposure to ISec threats or past actions, while primarily concentrating on direct experiences. Study 1 broadens the definition of prior ISec experience to encompass prior coping feedback and delves into the differential effects of direct and vicarious experiences on user cognition and behavior. Our findings reveal that threat appraisal mediates the effect of prior ISec incident exposure on protective intentions. Further, past coping behaviors shape protective intentions via a chain mediation process involving prior coping feedback and coping appraisal. Interestingly, vicarious experience influences user cognition and behavior in a manner akin to direct experience. Additionally, we offer insights into potential cognitive biases affecting the impact of individuals' prior experience on protective intentions. These findings bear significant implications for advancing both ISec research and practice.

3.1 Introduction to Study 1

As a key component of individual differences in PMT, PE is instrumental in forecasting intentions and behaviors (Safa et al., 2015), particularly for individuals lacking ISec training (Furnell et al., 2007; Thompson et al., 2017). Even trained individuals may exhibit irrational behavior due to the profound impact of PE on their decision-making process. For example, users previously unaffected by malware may underestimate future related threats. Moreover, despite having positive ISec protective intentions, individual users' actual ISec behaviors may not reflect their intentions. PE is the main reason that affects the stability between intention and behavior (S. Taylor & Todd, 1995). Thus, PE is an indispensable factor in understanding users' ISec issues, yet it has received limited attention in existing research.

Specifically, ISec related PE often appears as a control variable in most ISec behavioral research, which mainly refers to ISec threats experienced by users in the past (M Dupuis et al., 2012; Zahedi et al., 2015). It undoubtedly simplifies the abundant connotations of PE. Per PMT, when users encounter ISec threats, they will cope with them (either adaptive or maladaptive) and get feedback from coping activities (Rogers et al., 1997). This process will be stored in their episodic memory and can be used as information resources when similar threats recur (Atance & O'Neill, 2005; Schacter & Addis, 2007). However, limiting the definition of PE to only prior exposure to ISec threat experience fails to provide a complete picture of its impact on users. Moreover, in most ISec studies, the definition of PE is confined to the user's direct experience, which represents a narrow perspective. This is because prior vicarious experience (PVE), such as hearing or seeing others' ISec experiences, can also serve as PE that grants users access to knowledge they lack direct experience of (Bandura, 1977; Gino et al., 2010). Even when PVE emerges in some studies, it is often combined with prior direct experience (PDE) as a single variable labeled "past experience", which precludes understanding their potentially distinct effects (e.g., Mwagwabi et al., 2014).

Based on the above, Study 1 aims to investigate individual users' ISec related PE from theoretical and empirical perspectives, with insights relevant to practitioners and researchers. The article is structured as follows: Firstly, we review related studies, define ISec related PE, and propose hypotheses. Next, we present our research method and data analysis process. We then discuss research and practical implications, limitations, future research opportunities, and conclude.

3.2 Literature review and research gaps of Study 1

3.2.1 Prior experience in PMT and its role in ISec behavioral research

Prior experience often refers to something personally encountered before or the practical knowledge, skills, and practice obtained from observation or participation in events/activities in the past. PE is constructed through the active organization of the brain into episodic memories and is subsequently accessed when predicting and simulating future events in our mind (Bartlett, F. C., & Bartlett, 1995; Schacter & Addis, 2007). Within the framework of PMT, PE represents a crucial intrapersonal information source, encompassing previous threat exposure, past responses, and previous "feedback from coping activity" (Rogers et al., 1997, p. 114). PE will "force reappraisals of the threat and coping resources" (Rogers et al., 1997, p. 117), subsequently influencing individuals' intentions and actions. However, Rogers et al. (1997) highlight that certain facets of PE, particularly the aspect of prior coping feedback, remain inadequately examined in PMT research.

A review of PMT-based ISec literature resonates with this observation. A limited number of studies focus on prior ISec experiences, and as depicted in Table 2, the majority conceptualize prior experience merely as past exposure to ISec threats (Srisawang et al., 2015; Tsai et al., 2016). Few ISec articles measure individuals' prior responses to threats, such as prior habitual ISec policy compliance (Vance et al., 2012). Moreover, to our best knowledge, to date, no PMT-oriented ISec study has investigated feedback derived from past coping actions, suggesting a potential knowledge void regarding the influence of prior coping feedback on current cognitive and behavioral patterns. This omission may bias conclusions. For instance, if a user's PE conflicts with an ISec persuasive message, their interpretation may diverge from theoretical projections. Ignoring individuals' background differences, including PE, during ISec practice and implementing standardized ISec training may also be ineffective (Kim, 2013; Valentine, 2006). Although some ISec studies have tested PE as a control variable, the lack of in-depth exploration makes our understanding of PE inevitably limited. This is primarily evident in the discord between PE's broad scope and the narrow lens of ISec research.

TABLE 2 PMT-based ISec empirical studies involving prior experience

Study	Context	Definition of PE	Type of PE	Findings on PE
Anderson & Agarwal (2010)	Investigate the drivers of cyber citizens' intent to perform security behaviors, and interventions that can positively affect the drivers.	Prior experience with security violations, prior exposure to media coverage of security	Direct	Media exposure and prior experience with security violations were not significantly related to intentions.
Chai et al. (2009)	Examine factors that influence internet users' private information-sharing behavior.	Individuals' personal experience of personal information breaches or threatening safety on the internet.	Direct	Past experience has significantly negative impact on information privacy self-efficacy and protection intention.
Chen et al. (2017)	Study the antecedents of being an Internet scam victim and how it impacts online privacy concerns and privacy protection behaviors.	The experience of online privacy loss.	Direct	Past experience positively influences individuals' online privacy concerns.

Study	Context	Definition of PE	Type of PE	Findings on PE
Dupuis et al. (2012)	Check the home users' information security behavior in the context of backing up information.	Negative past experiences related to losing important information (include severity and frequency of the experience)	Direct	Someone with negative past experiences is more likely to overestimate the risk of losing information.
Haeussinger & Kranz (2013)	Propose a research model examining ISec awareness's antecedents and its mediating role.	Negative experience of being harmed directly or indirectly by any kind of information security incidents.	Direct and vicarious	Prior Negative Experiences with ISec incidents had a positive effect on ISA.
Hina et al. (2019)	Study the influence of institutional governance (IG) on protection motivation and planned behavior of employees in Higher education institutions.	An individual's personal or work-related ISec incident experience that raises long-lasting consciousness for future dealings.	Direct	Prior negative experience positively impacts self-efficacy but does not significantly impact threat appraisal.
Lee et al. (2008)	Develop and test a model of users' online protection behavior in the Internet virus context.	Previous virus infection experiences	Direct	Prior experience positively impacts virus protection intention.
Mousavi et al. (2020)	Explore the effectiveness of privacy assurance mechanisms in protecting SNS users from vendor-related privacy breaches.	Past privacy experience of information leakage	Direct	n.a.
Mwagwabi et al. (2014)	Examine how user views on passwords and security threats influence guideline compliance and ways to enhance this compliance.	Previous exposure to a hacking incident, experienced by either a user, or someone they know personally.	Direct and vicarious	Prior experience positively impacts perceived threat vulnerability.

Study	Context	Definition of PE	Type of PE	Findings on PE
Srisawang et al. (2015)	Investigate factors that affect computer crime protection behavior.	Past experience about computer crime threats, such as virus hits, computer security problems, breaches of privacy, etc.	Direct	Prior experience is significantly affecting threat appraisal.
Xin et al. (Xin et al., 2022)	Study the individuals' emotion-focused coping in the mobile malware context.	Previous exposure to similar ISec threats.	Direct	Prior experience does not impact protection intention.
Tsai et al. (2016)	Examine how classical and new PMT factors predicted users' online security intentions.	prior experience with virus infections.	Direct	Prior experience is significantly affecting protection intention.
Tu et al. (2015)	Explaining users' intent to mitigate damage from lost or stolen mobile devices.	Users' prior experience of device loss or theft	Direct	Prior experience positively impacts perceived threat.
Vance et al. (2012)	Influence of past routine IS security behavior on PMT's threat appraisal and coping mechanisms.	Routinized past ISec policy compliance behavior	Direct	Routinized past behavior positively impact both threat appraisal and coping appraisal.
Vance et al. (2013)	Examining how interactivity and fear appeals, both static and interactive, motivate users to strengthen their passwords.	Security incidents the participant has experienced in the past.	Direct	n.a.
Vance et al. (2014)	Comparing the predictive power of EEG measures with self-reported ISec risk perceptions, focusing on security warning disregard and risk perception changes before and after a security incident screen.	Past experiences with ISec incidents.	Direct	Participants with past experience have higher perceptions of ISec risk.

Study	Context	Definition of PE	Type of PE	Findings on PE
Zahedi & Chen (2015)	Examine how detection tools' performance and cost factors impact users' perceptions, efficacy against threats, and reliance on them.	Past encounters with fake websites	Direct	Past encounters positively impact perceived threat vulnerability.

3.2.2 A univocal understanding of PE in ISec behavioral research

According to Rogers et al.'s (1997) broadened definition of PE, when faced with ISec threats, individuals respond differently, including taking protective actions, continuing risky behaviors, or not responding at all (a form of maladaptive coping). Subsequently, they may receive feedback regarding their adaptive or maladaptive responses. All of which are stored as episodic memories and become an individual's PE (Bar, 2011; Norman & Reilly, 2003). This experience serves as an internal resource for individuals when facing similar threats in the future or when simulating potential threats (Rogers et al., 1997; Schacter & Addis, 2007).

However, most ISec studies only consider one aspect of PE, either previous threats (Srisawang et al., 2015; Tsai et al., 2016) or prior ISec behaviors (Vance et al., 2012). Previous feedback from responses remains largely unexplored (Rogers et al., 1997). This narrow focus fails to fully explain how PE affects individuals and may lead to conflicting research results. For instance, Hina et al. (2019) found that previous ISec incident experience did not affect participants' threat perception but positively impacted their self-efficacy—a finding at odds with numerous other studies (Rhee et al., 2009; Srisawang et al., 2015; Zahedi et al., 2015). This disparity might be attributed to participants in Hina et al.'s research effectively mitigating ISec incidents, thereby underestimating subsequent threats and gaining confidence in their coping capabilities.

3.2.3 PVE as part of PE

PVE is an important aspect of PE that enables individuals to learn from others, especially for those who lack direct experience in the ISec field (Bandura, 1977; Hanus, B., & Wu, 2016). This type of experience, obtained through others or media reports, serves as a vital source of information to fill knowledge gaps (Gino et al., 2010). While PMT doesn't explicitly encompass PVE, the theory's notion of observational learning parallels it, as both entail observing outcomes experienced by others (Bandura, 1977; Rogers et al., 1997).

Most ISec research only considers PDE, neglecting PVE. Some studies combine both sources of experience when measuring PE (Haeussinger & Kranz, 2013; Mwagwabi et al., 2014). However, various sources of experience can accumulate and impact individuals' perceptions of ISec threats, attitudes towards protective behaviors, and decisions differently over time (Fazio et al., 1982; Fazio

& Zanna, 1978). Unfortunately, the specific effects of ISec-related PVE on individuals' mental states and behavior are still uncertain.

3.2.4 Similarity in ISec related PE

When confronted with new problems, individuals are reminded of past situations that "bear strong similarity to the present problem (at different levels of abstraction)" (Carbonell, 1983, p. 1). Prior similar experience facilitate problem solving by allowing individuals to retrieve appropriate behaviors to meet the needs of the current situation, or to avoid repeating unfavorable experiences (Read & Grushka-Cockayne, 2011). PMT believes that PE with similar threats could invoke motivation to initiate the threat and coping appraisal processes (Rogers et al., 1997).

In short, the reasons above explain the disparity between the importance of ISec related PE and its knowledge gaps in ISec research. Therefore, a comprehensive inquiry into PE is imperative. Next, we will lay out the possible influence of prior ISec experience on individuals' subsequent cognitive processes and intentions.

3.3 Hypotheses development of Study 1

Under the mobile malware context, we derive two research models to study the role of PE grounded in the PMT framework. The model construction and related hypotheses will be discussed next.

3.3.1 The impact of threat and coping appraisals on behavioral intention across individuals with and without PE

Given that Chapter 2 provides a succinct overview of the hypothesized relationships between cognitive assessments and protection intention within the PMT framework and existing empirical evidence in ISec research, the hypotheses are presented here without further elaboration.

H1.1 Perceived threat severity of mobile malware predicts ISec protective intentions positively.

H1.2 Perceived threat vulnerability of mobile malware predicts ISec protective intentions positively.

H1.3 Response efficacy predicts ISec protective intentions positively.

H1.4 Self-efficacy predicts ISec protective intentions positively.

PE is one information source "capable of initiating cognitive activity leading to protective intention" (Milne et al., 2000, p. 108). The impact of cognitive factors on behavioral intentions may vary between those with and without PE. Evidence suggests that prior threat exposure leads to increased perceptions of threat severity and vulnerability (Srisawang et al., 2015; Tu et al., 2015; Zahedi et al., 2015), driving protective behavior (Tsai et al., 2016). This implies a stronger link between threat appraisal and protective intent in individuals with PE.

Perceived response efficacy and self-efficacy may have different relative influences depending on PE. Individuals without PE may pay place greater emphasis on response efficacy. They cannot adequately consider their ability to complete the coping actions in the formation of protective intention and instead focus on the effectiveness of coping strategies. Conversely, individuals who have experienced ISec accidents may have a weaker belief in their ability to deal with similar threats (Rhee et al., 2009). However, those who have demonstrated adaptive ISec behaviors in the past tend to perceive high response efficacy and self-efficacy (Vance et al., 2012). Thus, how individuals with PE perceive response efficiency and self-efficacy may require further consideration of the details of their PE. According to Taylor and Todd's (1995) study, perceived effectiveness of coping strategies was found to be the primary predictor of intentions among individuals with no PE, whereas those with PE exhibited reduced reliance on response efficacy and greater emphasis on self-efficacy. Based on the above, we hypothesize that,

H1.5 The relationship between ISec threat severity and protective intention is stronger for individuals with PE as compared to those without PE.

H1.6 The relationship between ISec threat vulnerability and protective intention is stronger for individuals with PE as compared to those without PE.

H1.7 The relationship between response efficacy and ISec protective intention is weaker for individuals with PE as compared to those without PE.

H1.8 The relationship between self-efficacy and ISec protective intention is stronger for individuals with PE as compared to those without PE.

3.3.2 The impact of PE on individual ISec behavioral intention with cognitive mediators and threat similarity moderation

Individual users' PE with information security can be divided into three main components: exposure to ISec threats, coping with these threats, and feedback received from coping activities (Rogers et al., 1997). Research has shown that PE has a direct impact on individual users' behavioral intentions (Ouellette & Wood, 1998), and this impact is also indirectly mediated by cognitive factors (Ajzen, 2002; Milne et al., 2000). Previous exposure to threats can affect individuals' cognition and intentions in two ways: severity of consequences and frequency of previous incidents. Previous studies suggest that such exposure can positively influence an individual's subsequent information protective intentions (Lee et al., 2008; Tsai et al., 2016). This victimization experience is considered a valuable source of knowledge that can influence one's perception of the current threat (Mwagwabi et al., 2014), leading to a generalized feeling of vulnerability and prompting “a broad array of self-protective behaviors”(Weinstein, 1989, p. 39). In addition, negative incidents also raise individuals’ future consciousness and interest in preventing similar incidents (Haeussinger & Kranz, 2013). Thus, we hypothesize that:

H2.1 Prior ISec incidents’ severity positively predicts ISec protective intentions, partially mediated by perceived threat severity.

H2.2 Prior ISec incidents’ frequency positively predicts ISec protective intentions, partially mediated by perceived threat vulnerability.

With this research scope, the term 'ISec threat similarity' denotes the degree of similarity between the ISec threats that individuals have encountered and the threats that they currently face (at different levels of abstraction). According to Kidwell and Jewell (2008), when an individual encounters a new problem situation, their threat appraisal will depend more on their previous experience if the past ISec threats are similar to the current ones. In such familiar situational conditions, the individual may rely less on evaluating attributes and more on the information previously learned in their environment. This suggests that individuals with PE may use similar situational information for threat appraisal instead of exerting cognitive effort to evaluate the current threats. For instance, an individual's perception of current malware threats might be informed by PE and factors encountered during previous malware infections. Thus, we hypothesize that:

H2.3 ISec threat similarity moderates the impact of PE of ISec incidents on threat appraisal; greater similarity amplifies the effect.

Previous ISec behaviors refer to any actions taken by an individual before in response to an ISec accident (e.g., mobile malware infection). Individuals estimate the possibility of future behaviors from their previous actions (Conner & Norman, 1995). Prior behavior exerts both a direct and an indirect effect on behavioral intentions, with the latter mediated by other determinants like cognition and external factors (Ouellette & Wood, 1998). Rippetoe and Rogers (1987) viewed past behavior as a distal influence mediated by coping appraisal. Thus, we hypothesize that:

H2.4 Prior adaptive ISec behaviors positively predict ISec protective intentions, partially mediated by coping appraisal.

Feedback regarding ISec related coping activities refers to the outcomes of individual users' previous responses to ISec threats, as well as their perceptions of these outcomes. Compared to maladaptive ISec behaviors, adaptive countermeasures are more likely to ensure users' information security and achieve the desired outcome (Liang et al., 2019). For instance, installing anti-malware software is more effective in defending against malware threats than taking no action. Moreover, feedback on past coping behaviors can affect individuals' final behavioral decisions (Albarracin & Wyer Jr, 2000). Thus, we hypothesize that:

H2.5 Prior adaptive ISec behaviors positively predict ISec protective intentions, partially mediated by the feedback of prior behaviors.

The decision to repeat coping behaviors is often influenced by individuals' prior coping experiences and feedback received. This effect is partly a result of cognitive processes (Albarracin & Wyer Jr, 2000). Specifically, in response to ISec threats, prior feedback on coping strategies serves as direct evidence of their effectiveness (Cervone, 2000). For example, whether anti-malware software successfully prevented malware intrusion affects one's assessment of its response efficacy. Moreover, prior performance and feedback received can affect one's self-efficacy judgment. In the ISec context, negative experiences such as a computer virus infection can lead to self-doubt and lower one's self-efficacy judgment. Conversely, successful PE can increase one's self-efficacy perception (Compeau & Higgins, 1995). Ultimately, individuals' perceptions of their response efficacy and self-efficacy influence their subsequent behavioral performance. Thus, we hypothesize that:

H2.6 The feedback of prior behaviors and coping appraisal play a chain mediation role in the process of prior behaviors affecting ISec protective intentions.

3.3.3 The impact of PDE and PVE on ISec behavioral intention

Individuals acquire knowledge from their own PE as well as from the experiences of others (Darr et al., 1995). PDE in the context of this study refers to the individual users' PE with ISec threats/accidents, responses, and feedback from responses. PVE refers to the ISec-related experiences that individuals acquire through various sources such as social communication and media, which have occurred to other individuals, including friends, relatives, neighbors, and even strangers (Kellens et al., 2011). PVE plays an important role in individual users' interpretation of information about ISec threats and defenses, in helping to understand the consequences of present ISec threats, and in decisions about whether to respond to threats. However, PVE impacts individuals' perceptions and behavioral intentions less than direct experience. In the healthcare context, scholars have found that individuals with vicarious cancer-related experience perceive lower risk and vulnerability and exhibit fewer behavioral changes than patients with direct cancer experience (Benyamini et al., 2003). Ashford et al. (2010) showed that PDE is the most powerful source to influence self-efficacy, followed by PVE. This is likely because PVE is less personalized and do not cement beliefs as profoundly as direct experiences (Achterkamp et al., 2016; Y. C. Lin et al., 2013). Thus, we hypothesize that:

H3.1 PVE has a weaker influence on ISec-related cognitive assessment and protective intention than PDE.

3.4 Research methodology in Study 1

This section describes the development of the measurement tool in Study 1, detailing its reliability and validity verification processes, alongside the methodology for data collection and analysis.

3.4.1 Measurement development and data collection in Study 1

Threat severity, threat vulnerability, response efficacy, self-efficacy, similarity of the threat and constructs of prior experience (i.e., severity of previously experienced threats, frequency of previously experienced threats, prior coping behavior, feedback of the prior coping behavior) were measured in this study. The multi-item scales for the study were developed from established theoretical frameworks and literature (Eppright et al., 2003; Milne et al., 2002; Rippetoe & Rogers, 1987; Witte, 1992, 1996), ensuring their relevance to the mobile malware context. To validate content, the study included a comprehensive literature review, a pre-test with an expert panel from the faculty of information and technology, and a meticulous questionnaire translation process for Chinese participants, following Del Greco et al.'s (1987) guidelines. This process involved initial translation, comparison for content and clarity, and cross-language equivalence testing with bilingual subjects. Additionally, a pilot study with a small subset of the target population was conducted to assess the questionnaire's comprehensibility and suitability for the larger study, verifying that, participants understood the questionnaire as intended. This pilot study was crucial for evaluating both the questionnaire's structure and the practicality of research procedures (Dillman et al., 2014).

A group of students and staff from a prominent Chinese university, representing a substantial segment of smartphone users, were chosen for a study. They participated in an anonymous online survey, conducted under supervisory guidance. For more details on the survey's structure and measurement items, please check Appendix.

Participants were invited to anonymously complete an online survey under supervisor oversight. They initially completed the survey which aimed to explore their current perceptions of mobile information security and their intentions to update their mobile operating system promptly. Subsequently, they were asked to provide their responses regarding their direct and vicarious PE with mobile malware-related threats. A checklist of malware symptoms was provided to aid in recalling and evaluating past occurrences.

From the 446 total responses, data cleaning procedures ensured the validity by excluding bogus responses and those completed under three minutes, the minimum time deemed necessary to complete the survey attentively (Meade & Craig, 2012). The online survey was also designed to ensure there were no missing values in the responses, and remove all the extreme values, resulting in a final dataset that included 425 usable observations, of which 66 had no PE, 254 had direct PE, and 105 had vicarious PE. The sample size met the rule of thumb requirement for structural equation modelling (Kline, 2011).

3.4.2 Data analysis and results of Study 1

The survey items' reliability and validity are evaluated, and hypotheses are tested using R 4.3.1 in this section. In Study 1, the control variables' impact on the research models is insignificant, hence, will not be further elaborated upon.

We conducted a confirmatory factor analysis to assess convergent and discriminant validities of the measurement. The factor loadings for the items exceeded 0.64 (Straub et al., 2004) and principal factor analysis supported convergent validity by showing all items loading on the posited construct at 0.78 or greater (Hair Jr et al., 2010). Higher item loadings within a construct and higher AVE values than inter-construct correlations confirmed discriminant validity (Straub et al., 2004). In addition, our measurement is highly reliable, with all constructs exceeding a Cronbach's alpha value of 0.80 and composite reliability scores above the cut-off value of 0.70 (Fornell & Larcker, 1981; Gefen & Straub, 2005; Nunnally et al., 1978). For more details, please check Table 3.

TABLE 3 Confirmatory and exploratory factor loadings including latent control variables

Constructs	Items	EFA Loading	CFA Loading	AVE	CR	Cronbach Alpha
Threat severity	Sev1	0.886	0.859	0.732	0.916	0.870
	Sev2	0.877	0.784			
	Sev3	0.837	0.755			
	Sev4	0.821	0.852			
Threat vulnerability	Vul1	0.875	0.870	0.718	0.910	0.877
	Vul2	0.874	0.821			
	Vul3	0.853	0.817			
	Vul4	0.784	0.694			
Response efficacy	Res1	0.911	0.869	0.719	0.911	0.916
	Res2	0.851	0.864			
	Res3	0.844	0.822			
	Res4	0.780	0.874			
Self-efficacy	Sel1	0.886	0.885	0.732	0.916	0.887
	Sel2	0.879	0.930			
	Sel3	0.864	0.808			
	Sel4	0.790	0.640			
Protective intention	Int1	0.830	0.885	0.761	0.905	0.897
	Int2	0.910	0.761			
	Int3	0.875	0.936			
Threat similarity	Sim1	0.950	0.950	0.813	0.929	0.944
	Sim2	0.911	0.955			
	Sim3	0.841	0.842			
Prior ISec incidents' severity	P_sev1	0.964	0.891	0.867	0.951	0.942
	P_sev2	0.928	0.973			
	P_sev3	0.901	0.900			
Prior ISec incidents' frequency	p_vul1	0.912	0.927	0.816	0.930	0.903
	P_vul2	0.901	0.925			
	P_vul3	0.897	0.762			
Feedback of prior coping	P_res1	0.976	0.960	0.914	0.969	0.960
	P_res2	0.955	0.941			
	P_res3	0.936	0.930			
Important information on the mobile	Assim1	0.930	0.923	0.867	0.952	0.922
	Assim2	0.925	0.908			
	Assim3	0.939	0.932			

Procedural and statistical remedies were used to reduce the risk of common method bias in this dissertation. In terms of procedural remedies, each item was made concise and straightforward in verifying the content validity by avoiding unfamiliar terms and vague concepts (Tourangeau et al., 2000). The anonymity of participants was protected to reduce social desirability bias. Additionally, the order of measurement of independent variables and the dependent variable was balanced to control biases related to the items' embeddedness (Tehseen et al., 2017). In terms of statistics, the correlation matrix of latent variables did not reveal any large correlations (r<0.9). Harman's one-factor test was also used to evaluate the model. Ten factors with eigenvalues greater than 1 explained 83% of the data variance in exploratory factor analysis without rotation. The first factor explained only 26.09% of the variance, accounting for 31.43% of the total variance, falling short of the 25-50% range recommended by Hair Jr et al. (2010). It suggests that CMV was not a significant issue in the data.

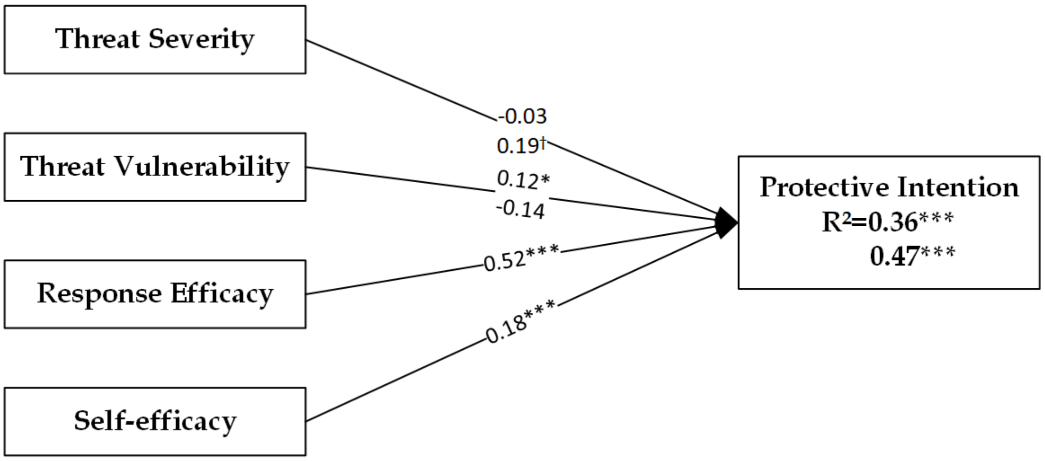
We employed the maximum likelihood method and multigroup analysis to estimate and compare the models examining the influence of cognitive factors on behavioral intentions among individuals with and without PE, to test hypotheses H1.1 to H1.8. The estimation results are presented in Figure 2, and all fit indices of the structural model met the cut-off threshold proposed by Hooper, Coughlan, and Mullen (2008), indicating an acceptable model. The statistical significance of the R-squared values for the endogenous variables (as shown in Figure 2) indicates that the model has a reasonable explanatory power.

As shown in Table 4, most path coefficients for both groups (with and without PE) were significant. Specifically, perceived threat severity had a significant positive effect on protective intention among users without PE, while perceived threat vulnerability had a significant positive effect on protective intention among experienced users. Coping efficacy and self-efficacy had significant positive effects on intention as expected in both groups. Therefore, H1.1 to H1.4 was largely supported.

A comparison of the models for individuals with and without PE revealed that H1.6 was supported, suggesting a higher correlation between perceived threat vulnerability and protective intention for users with PE compared to those without PE. In contrast, H1.5 and H1.8 yielded results that were opposite to expectations, indicating that the effects of threat severity and self-efficacy on protective intention for users without PE were greater than those for users with PE. The difference in the impact of response efficacy on protective intention between the two groups was not found to be statistically significant.

TABLE 4 Wald χ2 Tests for Significance of Path-Coefficient Differences among individuals with and without PE

Path	**Path Coefficient**		**Δχ2**	**Sig.**
	With PE	Without PE		
Threat severity → Protective intention	-0.03	0.19†	2.85	0.09†
Threat vulnerability → Protective intention	0.12*	-0.14	4.50	0.03
Response efficacy → Protective intention	0.52***	0.40**	0.08	0.78
Self-efficacy → Protective intention	0.18**	0.45***	3.97	0.04



Note: *p≤0.05, **p≤0.01, ***p≤0.001, † 0.05≤p≤0.1. Path coefficients are on arrow lines, top value = users with PE, bottom value = users with no PE

FIGURE 2 Results of cognitive Assessment effects on individuals' protection intention: with PE vs. with no PE

Monte Carlo simulations is conducted to estimate standard errors and confidence intervals for mediation effects, with 5,000 iterations. We established a moderated mediation model to examine the impact of ISec related PE on individuals' protective intentions, mediated by threat appraisal and moderated by threat similarity. The SEM analysis revealed that perceived threat severity significantly mediates the impact of the severity of prior ISec incidents experience on individuals' protective intention in the direct PE group, thereby confirming H2.1. Similarly, the frequency of prior ISec incidents significantly affects protective intention in the direct PE group, mediated by threat vulnerability, verifying H2.2. No mediation effect is observed in the vicarious PE group, but the severity of prior ISec incidents experience directly influences both the perceived threat severity and protective intention. The interaction between threat similarity and the severity of prior ISec incidents experience is significant (0.156, p=0.01) in the PDE group, indicating that threat similarity strengthens the influence of prior ISec incidents' severity on perceived threat severity. However, there was no discernible moderating influence of threat similarity on the association between the frequency of prior ISec incidents and perceived threat vulnerability in both analyzed groups. Thus, H2.3 is partially supported. Finally, we examined the moderated mediation effect and found that the conditional indirect effects of prior ISec incidents experience are not significant.

In addition, we explore the impact of past behavior on protective intention, examining the mediating factors of coping appraisal and prior coping feedback individually. Our results indicate a noteworthy and positive influence of past behavior on protective intention, partially interpreted by coping appraisal and prior coping feedback in both direct and vicarious PE groups. Hypotheses 2.4 and 2.5 are supported.

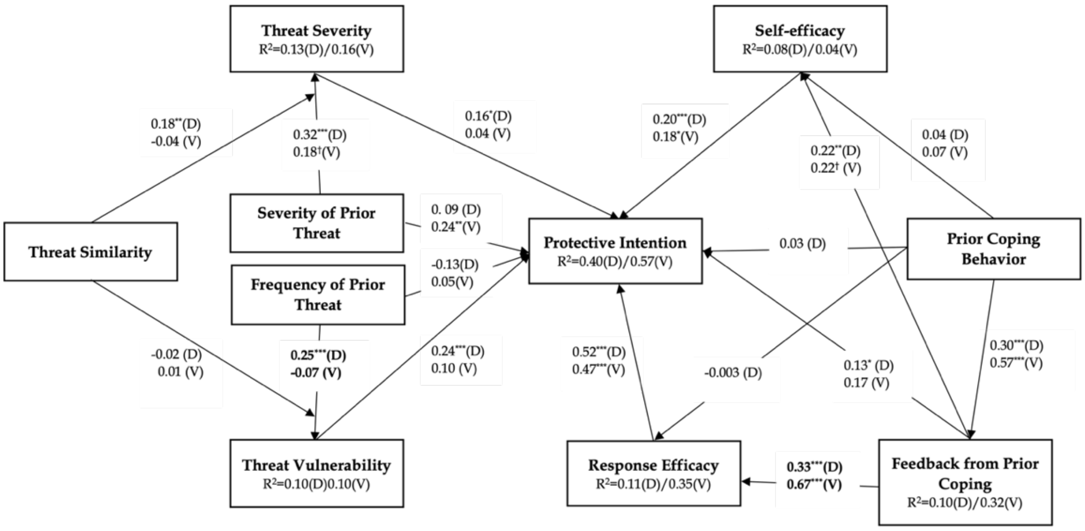
We also explored the chain mediating effect in the model. As presented in Figure 3, our results indicate that past behavior indirectly influences protective intention through prior coping feedback and response efficacy in both analyzed groups. The chain mediating effect of prior coping feedback and self-efficacy between past behavior and protective intention was also significant. Therefore, we can confirm H2.6. Please check Table 5 for more details.

TABLE 5 The mediating effect of cognitive assessment and feedback of prior coping on the relationship between PE and ISec protective intention

Mediating path	**Group**	**Indirect effect**	**SE**	**P-value**	**95% CI**
Severity of prior ISec incidents → Threat severity → Protective intention	PDE	0.053	0.026	0.044	0.001, 0.104
	PVE	0.007	0.019	0.731	-0.031, 0.044
Frequency of prior ISec threat → Threat vulnerability → Protective intention	PDE	0.065	0.026	0.014	0.013, 0.116
	PVE	-0.007	0.012	0.578	-0.031, 0.017
Prior coping behavior → Feedback from prior coping→ Protective intention	PDE	0.463	0.110	0.000	0.247, 0.679
	PVE	0.771	0.201	0.000	0.378, 1.164
Prior coping behavior → Response efficacy → Protective intention	PDE	0.264	0.128	0.039	0.134, 0.515
	PVE	0.368	0.154	0.017	0.067, 0.668
Prior coping behavior → Self-efficacy → Protective intention	PDE	0.173	0.083	0.038	0.010, 0.336
	PVE	0.207	0.101	0.040	0.010, 0.404
Prior coping behavior → Feedback from prior coping → Response efficacy → Protective intention	PDE	0.270	0.092	0.003	0.103, 0.472
	PVE	0.405	0.129	0.002	0.170, 0.669
Prior coping behavior → Feedback from prior coping → Self-efficacy → Protective intention	PDE	0.132	0.059	0.027	0.035, 0.270
	PVE	0.085	0.056	0.100	0.000, 0.220

Through a Wald χ2 test, we investigated the varying influences of prior direct and PVE on protective intention. Our analysis revealed that significant differences exist between the two groups of subjects in terms of the impact of prior ISec incidents' frequency on threat vulnerability and the impact of prior coping feedback on response efficacy. Specifically, the frequency of prior ISec incidents in the PDE group better predicts the subjects' perception of threat vulnerability (Δχ2=7.57, p=0.006), whereas the prior coping feedback in the PVE group has a stronger impact on response efficacy (Δχ2=9.46, p=0.002). There were no significant differences in other path coefficients between the two groups.

The t-test comparison of mediating effects in two groups revealed that the mediating effects of threat appraisal on the relationship between the experience of prior ISec incidents and protective intentions were not significant in the PVE group, but significant in the PDE group. Perceived coping appraisal and prior coping feedback had significant mediating and chain mediating effects on the relationship between past behavior and protective intention, and their mediating effects were not significantly different between two groups. Therefore, only the path from prior threat frequency to threat vulnerability verifies H3. Table 6 summarizes the hypothesis verification results of Study 3.



Note: *p⩽0.05, **p⩽0.01, ***p⩽0.001, † 0.05⩽p⩽0.1. Path coefficients are on arrow lines, top value = users with PE, middle value = users with direct PE (D), bottom value = users with vicarious PE (V).

FIGURE 3 Results of the impact of PE on individuals' ISec Protective Intention: Direct vs. Vicarious

TABLE 6 Summary of Hypotheses

Hypotheses	Supported
H1.1: Perceived threat severity positively predicts ISec protective intentions.	Partial
H1.2: Perceived threat vulnerability positively predicts ISec protective intentions.	Partial
H1.3: Response efficacy positively predicts ISec protective intentions.	Yes
H1.4: Self-efficacy positively predicts ISec protective intentions.	Yes
H1.5: The relationship between threat severity and protective intention is stronger for individuals with PE as compared to those without PE.	No
H1.6: The relationship between threat vulnerability and protective intention is stronger for individuals with PE as compared to those without PE.	Yes
H1.7: The relationship between response efficacy and protective intention is weaker for individuals with PE as compared to those without PE.	No
H1.8: The relationship between self-efficacy and protective intention is stronger for individuals with PE as compared to those without PE.	No
H2.1: Prior ISec incidents' severity positively predicts ISec protective intentions, partially mediated by perceived threat severity.	Yes
H2.2: Prior ISec incidents' frequency positively predicts ISec protective intentions, partially mediated by perceived threat vulnerability.	Yes
H2.3: ISec threat similarity moderates the impact of PE of ISec accidents on current threat appraisal; greater similarity amplifies the effect.	Partial
H2.4: Prior adaptive ISec behaviors positively predict ISec protective intentions, partially mediated by coping appraisal.	Yes

Hypotheses	Supported
H2.5: Prior adaptive ISec behaviors positively predict ISec protective intentions, partially mediated by the feedback of prior behaviors.	Yes
H2.6: Behavioral feedback and coping appraisal play a chain mediation role in the process of prior behaviors affecting ISec protective intentions.	Yes
H3.1: PVE has a weaker influence on ISec-related cognitive assessment and protective intention than PDE.	Partial

3.5 Discussion of Study 1

Study 1 comprehensively investigates the role of PE in individuals' information security performance, structured into three main sections. Initially, we compared the ISec protective intentions of individuals with and without PE. Subsequently, we studied the mechanisms through which PE influence an individual's protective intentions. Finally, we contrasted the impact of PVE versus PDE on individuals' protective intention.

3.5.1 Key Findings in Study 1

Study 1 comprehensively investigates the role of PE in individuals' information security performance, structured into three main sections.

First, we examined and compared the influence of cognitive factors on participants' protective intentions regarding information security, considering their ISec related PE. Our findings suggest that individuals' perceptions of coping strategy effectiveness and their self-efficacy play crucial roles in influencing ISec behaviors, independent of participants' PE. This finding corroborates behavioral change theories and aligns with preceding ISec research (Ajzen, 1985; Rogers et al., 1997; Yoon & Kim, 2013; Zhang et al., 2017). Threat appraisals significantly and positively affected protective intentions, although patterns varied depending on participants' PE. As expected, individuals with PE exhibited heightened sensitivity to potential risks and vulnerabilities associated with information security, thereby strengthening their protective intentions. On the other hand, inexperienced users were more susceptible to the severity of potential ISec threats, motivating them to take protective measures. This finding contradicts our hypothesis, possibly because people without PE may be more sensitive to novel or unfamiliar threats. The novelty factor can amplify the perceived impact of a potential threat (Hopp & Gangadharbatla, 2016), thus enhancing their perception of threat severity and its impact on protective intentions. However, previous exposure to a particular ISec threat reduces the subsequent impact of the same or similar threats, as "direct tolerance" (Norris & Murrell, 1988), thus lowering the individuals' threat severity assessment.

Another result, contrary to our hypothesis, is that users new to ISec issues may rely more on their beliefs about self-efficacy when forming protective intentions compared to users with PE. This may be because users without PE perceive risk and uncertainty when dealing with unknown threats. In such cases, higher self-efficacy can provide a sense of control and self-confidence, alleviating individuals' perception of uncertainty (C. C. Chen & Greene, 1998; Krueger & Dickson, 1994). Consequently, individuals may place greater weight on their self-efficacy beliefs to shape their intentions to act protectively.

Interestingly, we found no significant difference in perceptions of the effectiveness of protective measures in mitigating ISec threats between individuals with and without PE. Individuals with prior ISec-related experience may have acquired knowledge and skills related to protective measures, which aid their understanding of response efficacy. However, knowledge and understanding of effective protective measures are not limited to individuals with PE. Information on effective security practices is widely available through various sources, such as educational resources, industry standards, and guidelines. This knowledge is equally accessible to individuals without PE, influencing their perception of response efficacy in a similar manner.

Second, we examined the impact of PE on cognitive factors and protective intentions. Our findings from Study 1 indicate that threat appraisal mediates the link between PDE of ISec incidents and protective intentions. Individuals with previous exposure to ISec incidents perceive higher risk severity, increased vulnerability to future threats, and demonstrate stronger protective intentions. In contrast, the mediating effect of threat appraisal was not observed in the group with only vicarious experiences. Nonetheless, individuals who have encountered ISec incidents indirectly still perceive threats as severe and exhibit protective intentions based solely on vicarious experiences.

ISec threat similarity plays a crucial role in shaping the relationship between prior exposure to ISec incidents and threat severity perception. In cases where individuals perceive a high level of resemblance between their previous exposure with ISec incidents and anticipated threats, the severity of past events exerts a more pronounced impact on their perception of threat severity. However, we did not observe a discernible moderating influence of threat similarity on the association between the frequency of prior ISec incidents and perceived threat vulnerability, for both direct and vicarious PE groups. These findings imply that the frequency of prior ISec incidents may have a more direct and consistent impact on perceived vulnerability, regardless of the level of perceived threat similarity. One possible explanation is that the severity of previous exposure serves as a prominent reference point for individuals when they encounter a threat similar to their PE, thereby amplifying the impact on their perception. Conversely, the frequency of previous threat experiences may not exhibit the same significance or direct correlation with current vulnerability perceptions. This implies that the relationship between PE and current vulnerability perceptions is likely driven more by the frequency of exposure to threats or problems rather than the similarity of threats or problems. For instance, an individual with multiple exposures to malware may perceive a higher likelihood of being attacked by various types of malwares in the future, irrespective of whether the malware itself or the circumstances leading to the infection are similar.

Moreover, the impact of previous ISec-related behaviors on protective intentions is mediated by two factors: prior behavioral feedback and coping appraisals. When individuals have previously engaged in adaptive ISec behaviors, they tend to receive positive feedback on their outcomes and develop a belief in the efficacy of countermeasures, as well as their own capability to handle threats. These factors, in turn, foster an increased willingness to protect. By exploring the chain mediation effect of prior behavioral feedback and coping appraisals, we uncover the mechanism through which prior behaviors shape protective intentions. This mechanism involves the dissemination of positive outcomes derived from adaptive behaviors in response to ISec threats. Consequently, individuals' beliefs in the effectiveness of countermeasures and their self-efficacy are strengthened, leading to heightened protective intentions. Likewise, vicarious experiences impact perceived coping efficacy, self-efficacy, and protective intention, as individuals are influenced by the observations or narratives of others' previous behavioral responses and coping outcomes.

Finally, our study compared effects of direct and vicarious experiences on individual cognitive factors and protective intentions related to information security. Individuals with experience of direct exposure to ISec incidents believed in a higher likelihood of future ISec threats compared to those who frequently heard or witnessed others facing such incidents. This finding aligns with our expectations, highlighting the significant role of first-hand experience in shaping individuals' understanding of vulnerability to ISec-related risks. Surprisingly, coping feedback from prior vicarious experiences had a stronger influence on response efficiency than direct experiences. This implies that individuals who observe or hear about others successfully dealing with ISec threats are more likely to perceive adaptive countermeasures as effective. This effect may be attributed to the credibility of information sources (Jones et al., 2003; Pornpitakpan, 2004). Prior vicarious experiences may provide social evidence of the effectiveness and success of coping strategies against ISec threats, especially when the prior coping feedback comes from highly credible sources, such as experts or trustworthy peers (Pornpitakpan, 2004). In addition to the aforementioned differences, there were no significant variations in the path coefficients between the PDE and PVE groups. It suggests that the influence of prior ISec behaviors on future intentions relies on behavioral feedback and beliefs in coping strategy effectiveness and self-efficacy, regardless of direct or vicarious experiences. Several possibilities could account for these findings. For instance, individuals may interpret and internalize their experiences differently. Those with direct experiences may have encountered specific impactful ISec events that strongly influenced their perception of ISec threats and intentions. While vicarious experiences offer individuals a broader understanding through exposure to diverse information sources. The subjective interpretation and weighting of experiences may contribute to the convergence of results between the two groups. The timing and recency of PE may also contribute to these results

(Perugini & Bagozzi, 2001). Individuals who have directly experienced information security incidents may have encountered more significant events in the past, whereas those who have had indirect experiences might have recently been exposed to related events. If there is a substantial temporal gap between prior direct experiences and individuals' cognitive assessments and protective intentions, the impact strength may diminish, resulting in similar outcomes to those with vicarious experiences (Messier et al., 1994).

3.5.2 Contributions to research in Study 1

Study 1 emphasis the importance of ISec related PE and provides comprehensive insights into its influence on information security performance by developing a more comprehensive model of ISec related PE, makes three main contributions to the research.

Study 1 expands the conceptualization of prior ISec experience and constructs a model that clarifies how PE influences individuals' cognition and behavioral intention, and providing a comprehensive explanation of its impact. Much of the existing ISec research based on behavioral change theories tends to overlook or narrowly define PE, often limiting it to previous exposure to ISec threats or past behavior, providing simplistic summaries of its effects. Study 1 addresses these limitations by positing that PE encompasses the entire process of an individual's encounter with an ISec incident, ranging from its occurrence to its resolution. This integrated perspective incorporates three crucial factors: prior exposure to ISec threats, previous responses, and feedback received from those responses. Notably, the investigation of feedback from previous behaviors in the ISec field is a novel contribution of this study.

Using the context of mobile malware threats as the example, our study indicates that users, when previously exposed to similar serious threats, tend to perceive potential mobile malware as severe. And the frequency of previous exposure would lead users to believe that they are more likely to be targeted by mobile malware threats, thereby enhancing their motivation to protect mobile information security. Additionally, users who have previously employed positive coping strategies in ISec incidents are more likely to exhibit the protective behaviors in the future. This is because positive coping strategies are likely to yield positive feedback, such as successfully removing detected malware following the instructions provided by antivirus software. Positive behavioral feedback further reinforces users' belief in the effectiveness of coping with ISec threats and their confidence in effectively handling ISec crises, thus increasing the likelihood of engaging in similar protective behaviors in the future. Our study highlights the importance of prior ISec experience in shaping individuals' protective intentions in the context of information security.

Second, this paper enriches the existing literature by investigating the role of PE, both direct and vicarious, in shaping protective intentions - a topic often overlooked in ISec studies. By addressing this gap, our study responds to Haag et al.'s (2021) call for more research on the influence of PE. Our research revealed that the positive impact of response efficacy and self-efficacy on the intention to protect mobile phone information security remains significant and stable, irrespective of prior ISec-related experience. However, users frequently exposed to ISec threats perceive a higher vulnerability to mobile malware attacks than those who learn about such incidents from others. Those without any PE perceive the least threat vulnerability, resulting in lower protective intentions.

In addition, some unexpected findings also show us the role of factors such as cognitive biases in shaping the impact of PE on individual cognition and intention. For example, we discovered that individuals without PE perceive mobile malware infection consequences as severe, fostering stronger protective intentions. Conversely, those with PE exhibit reduced threat sensitivity. It is likely attributable to the novelty effect, which refers to the heightened stress response individuals typically exhibit when first encountering a potential threat and diminishes over time as the novelty subsides (Hopp & Gangadharbatla, 2016). Another interesting result is, individuals without PE display greater confidence in their ability to handle mobile malware threats, suggesting an optimism bias. This bias could cause them to place undue reliance on their self-efficacy beliefs, presuming their skills and knowledge are adequate to counter any risks (S. E. Taylor et al., 1992; Weinstein, 1980). Additionally, compared to successfully dealing with threats themselves, hearing about others successfully managing ISec incidents can enhance individuals' belief in their response efficacy, potentially due to the halo effect or authority bias (Djafarova & Rushworth, 2017). When information comes from what individuals perceive to be expert or trustworthy sources, this bias may influence how they perceive information related to ISec threats. In recent years, cognitive bias has been demonstrated to have a non-negligible impact on individual decisions or behaviors related to information security, reflecting the irrational thinking aspect of human decision-making and action-taking (Fleischmann et al., 2014; Tsohou et al., 2015). These findings underscore the need for further research into the role of cognitive biases in shaping individual information security behaviors.

Finally, this study enriches our understanding of the relationship between PE and ISec protective intentions by exploring the mediating roles of prior behavioral feedback and cognitive factors, and the moderating role of prior threat similarity. It underscores the significance of mediation and moderation in theory testing and development. While cognitive mediation is a fundamental assumption of behavior change theories like PMT (Milne et al., 2002), which can provide important information for theoretical testing, but it has been ignored in both theoretical elaboration and empirical verification in ISec research (Xie, 2022). Our study addresses this gap by showing that threat and coping appraisals mediate the link between PE and intentions, thereby reinforcing the theory's underlying assumptions. The moderating role of threat similarity between previous ISec events and threat severity perceptions further illuminates the complexity and contingency of their relationship, contributing to theory development. We also demonstrate the chain mediation role of prior behavioral feedback and coping appraisal, a methodological contribution to information security behavioral research. By examining the chain mediation effect, we illustrate the sequential relationship between prior ISec coping behavior, behavioral feedback, coping appraisal, and protective intention, thereby uncovering specific transmission mechanisms. Quantifying each mediator's indirect impact clarifies their relative importance, with our study revealing a more significant role for prior behavioral feedback. In conclusion, identifying and validating specific mediating processes enhances our understanding of the psychological and behavioral processes related to individual information security. This leads to theoretical advances, model improvement, and the generation of new research questions.

3.5.3 Implications of Study 1 for practice

First, our research from Study 1 significantly aids ISec professionals by elucidating the impact of PE on individuals' current perceptions, choices, and intentions in information security. This study offers valuable reference data for crafting ISec educational programs and training. Although some researchers assert the unchangeable nature of PE makes it a lesser testing variable(Ajzen, 1987), we propose it as a crucial predictive factor for individuals' present and prospective ISec behavior. Particularly, users lacking system ISec education may heavily rely on PE (Thompson et al., 2017). Consequently, tailoring ISec programs based on the target audience's PE can streamline security strategies.

Second, our research from Study 1 integrates prior coping feedback and vicarious experiences to better understand their impact on information security behaviors. Traditionally, research has mainly focused on prior direct experience, and often overlooking feedback from past behavior. Our study expands this scope, assessing how PE influence user behavior intentions. Findings indicate that adaptive coping feedback significantly enhances individual intention to defend against mobile malware. However, immediate, or short-term feedback of outcomes is often lacking for many information security (ISec) behaviors such as regular data backup and password changes. To address this, we suggest organizations implement feedback mechanisms that positively reinforce adaptive ISec behaviors, potentially through incentives or recognition. Moreover, our research demonstrates that vicarious experiences strongly influence perceptions of coping efficacy and protective intentions, with feedback from these experiences having a more substantial impact on response efficiency than direct experience. Therefore, organizations could capitalize on this by disseminating success stories and case studies of effective ISec threat management.

Third, Study 1 provides valuable insights into how an individual's past experiences can influence their commitment to regularly updating their mobile phone operating system, with an emphasis on mediation and moderation analysis. This insight holds practical value in formulating and refining Information Security (ISec) intervention strategies. Through identifying the sequential mediation process involving past coping feedback and coping appraisal, professionals can customize interventions, potentially leading to desired shifts in users' ISec protective actions. Notably, the substantial mediating effect of prior behavioral feedback implies that ISec intervention developers should prioritize this aspect to achieve desired outcomes. For instance, during organizational ISec exercises, allocating more resources to behavioral feedback could foster efficient ISec practices. Offering immediate positive feedback for adaptive coping behaviors reinforces their effectiveness and feasibility, while warnings for maladaptive behaviors highlight potential serious consequences.

3.5.4 Limitations of Study 1 and future research

This research in Study 1 possesses inherent limitations. First, its conclusions may not be fully applicable to smartphone users of different demographics and locales since it is drawn from a Chinese sample set, thus constraining the generalizability of the findings. Second, the study's examination of participants' PE rests on their subjective interpretations. The potential for disparate interpretation and internalization introduces variability that may not be adequately accounted for in the results. Additionally, the temporal proximity of PE to individuals' cognitive evaluations and protective intentions was not considered. As such, a significant temporal distance may reduce the influence of PE, potentially leading to an underestimation of their impact. Lastly, the study's applicability is restricted to malware threats, as a comprehensive review of all ISec threats is impracticable within a single study. For future research, we propose the expansion of sample diversity and consideration of different ISec threats. The utilization of experimental methods combined with longitudinal studies could help mitigate potential temporal influences and the bias inherent in self-reporting.

3.6 Conclusion from Study 1

Study 1 scrutinizes the pivotal role of Information Security (ISec) related PE in behavioral change theories. Our understanding of PE encompasses both direct and vicarious encounters, incorporating exposure to ISec incidents, previous behavioral responses, and coping feedback. The research expalins the mechanism through which PE shape future behavioral intentions. Experiencing ISec incidents heightens individuals' perception of risk severity and susceptibility, consequently shaping their behavioral intentions. Successfully addressing prior ISec threats augments the belief in countermeasures' effectiveness and self-efficacy, promoting the adoption of similar coping behaviors in future encounters. Vicarious ISec experience shares a comparable influence on cognitive and behavioral molding as direct experience. This research significantly contributes to the field of individual user information security behavior, bridging the existing knowledge gap in ISec research concerning PE.

4 STUDY 2: HOW USERS CONSTRUCT INFORMATION SECURITY FEAR APPEALS AT THE COGNITIVE LEVEL: PSYCHOLOGICAL DISTANCE AND CONSTRUAL LEVEL EXPERIMENT

Designing effective fear appeal messages is a critical component of ISec behavioral research. Despite advancements, the cognitive processes by which users interpret these messages—termed mental representations of fear appeals—remain insufficiently theorized and explored. This research gap hampers our understanding of the theoretical mechanisms linking fear appeal messages to users' mental states and subsequent behaviors. Leveraging Construal Level Theory (CLT), this study examines how users' mental representations of fear appeals influence their subsequent cognitive evaluations. Experimental results within an anti-malware framework indicate that both low construal levels and proximal psychological distances of ISec threats in the fear appeals generate specific mental representations, enhancing users' threat appraisals and intentions to adopt recommended actions. These findings illuminate the pivotal role of mental representations in shaping users' responses, offering new avenues for both researchers and practitioners to influence user behavior more effectively.

4.1 Introduction to Study 2

Defined as persuasive messages emphasizing adverse consequences of noncompliance, fear appeals usually present a threat description and remedial advice (Milne et al., 2000), which serve as one strategy to influence individuals' ISec intentions and behaviors (Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010). Cognitive psychology posits that individuals' perceptions and evaluations of ISec threats in fear appeals, as well as their subsequent behavioral intentions, stem from how they construct the threat at the cognitive level

(Sterelny, 1990; Von Eckardt, 2012). In ISec research, scant attention has been given to the cognitive construction of threat within fear appeals, particularly the intermediary process that translates message cues into individual evaluations. This cognitive gap, termed as 'mental representations' in cognitive psychology, remains largely unexplored in the literature. The concept of mental representation is crucial in ISec, as it illuminates the 'black box' between the fear appeal message and subsequent mental states, especially when dealing with threats that are intangible as opposed to directly observable threats like fire (cf., Karjalainen & Siponen, 2011). Moreover, the challenge does not lie only in the intangibility of ISec threats. ISec threats are human-made, and they are often designed to work under the radar of users, unless the aim is, for example, to blackmail users, as seen in ransomware. In such cases, users mentally represent the inexperienced ISec threats (Sternberg & Sternberg, 2011). How individuals form images of ISec threats in their minds can have implications for how they respond to the fear appeal stimulus, and cognitive psychology is a critical part of understanding this. Cognitive psychology sees that individuals' evaluations, perceptions, and ideas of things that are abstract, do not currently exist, or have never been experienced, are processed through mental representations (Pitt, 2000; Sternberg & Sternberg, 2011). Consequently, an understanding of mental representation holds significant implications for the effective design of fear appeals.

Study 2 leverages CLT from cognitive psychology to investigate how mental representations influence the effectiveness of fear appeals. CLT posits that individuals process fear appeals at varying abstraction levels, which can further influence their threat assessment, decision-making, and intentions. We also examine how psychological distance from the ISec threat can affect these mental states. The empirical study aims to assess CLT's utility in designing more effective fear appeals for mobile malware contexts.

The rest of Chapter 4 is organized as follows. Sections 4.2 and 4.3 introduce background concepts, review related research, and put forward research hypotheses and models. In Section 4.4, the research method and data analysis are presented to test the hypotheses. The overall discussion, research contributions and limitations, and future research directions are included in the final sections.

4.2 Literature review and research gaps of Study 2

This section presents the theoretical background of individuals' mental construal of fear appeal messages, as well as the current state of research and the shortcomings of ISec related fear appeals.

4.2.1 Mental representation

Mental representation is the representation of the brain of “things that are not currently seen or sensed by the sense organs” (Mccarthy, 2018, p. 174). For example, when one is asked to recall one’s own experience of a malware threat, one might mentally reconstruct the situation by recollecting the consequences of the malware or the place where it happened though the threat is not presently visible. Mental representation also "enables representing things that have never been experienced as well as things that do not exist" (Sternberg & Sternberg, 2011, p. 276). One can think of experiencing the malware threat in one’s mind even if one has never experienced it. Mental representation “acts as intermediaries between the observing subject and the objects observed in the external world, which symbolize or represent the objects of this world” (Mccarthy, 2018, p. 175). People can engender mental states of things, such as thoughts, perceptions, beliefs, and intentions, based on their mental representations of things (Fodor, 1975, 1985; Williams, 1984). For example, when users believe that their password needs to be changed for security reasons (a mental state), they have formed a mental representation of the password and its state of security.

Examining mental representations in Information Security (ISec) research is particularly salient when addressing threats that are often less tangible than observable physical risks. Utilizing these mental constructs can enhance the efficacy of fear appeals in shaping individuals' perceptions of such threats.

4.2.2 Construal level theory and psychological distance

CLT explains how people perceive and evaluate things that are not present through mental representations (Dhar & Kim, 2007; Y Trope & Liberman, 2010). It assumes that individuals’ mental representations of cognitive objects have different degrees of abstraction, called construal level. Construal levels are influenced by individuals’ perceptions of psychological distance with the cognitive object (Y Trope & Liberman, 2010). Psychological distance is a subjective psychological perception that objects or events are close or far away from the self, here and now; the reference point is egocentric (Liberman, Trope, & Stephan, 2007; Y Trope & Liberman, 2010).Psychological distance includes four dimensions: (1) Temporal distance, (2) Spatial distance, (3) Social distance, and (4) Hypotheticality (Liberman, Trope, & Stephan, 2007; Liberman, Trope, & Wakslak, 2007; Liberman & Förster, 2008). Table 7 summarizes the operational definitions of psychological distance to ISec threats or information and data.

TABLE 7 Operational definitions of the psychological distance to ISec threats

Psychological distance	Operational definition
Temporal distance	An individual's subjective psychological perception that the time of the occurrence of an ISec threat is close to or far away from now.
Spatial distance to ISec threat	An individual's subjective psychological perception that the location where the ISec threat may happen is close to or far away from here.
Spatial distance to information/data	An individual's subjective psychological perception that the information, data, and systems are close to or far away from here.
Social distance	An individual's subjective psychological perception that someone who is exposed to ISec threats is close to or far away from themself.
Hypotheticality	An individual's subjective psychological perception that the likelihood of an ISec threat occurring or that the ISec threat is close to or far from reality.

Per CLT, users mentally represent ISec threats that are psychologically near in terms of low-level, detailed, and contextualized features. Conversely, they represent the same ISec threats that are mentally distant in terms of high-level, abstract, and stable characteristics. High construal levels of ISec threats are related to their "core" features, namely the nature of the damage or adverse effects that they cause. For example, the high-level feature of ransomware is that it is harmful. In turn, a low construal level of ISec threats represents their detailed characteristics. Low-level characteristics of ransomware could involve, for example, encrypting users' files to make them inaccessible and then demanding payment to decrypt them.

4.2.3 Fear Appeals in Information Security Literature

Fear appeals are strategically crafted messages aimed at inducing compliant behavior by detailing the severity of potential threats (Witte, 1992). These messages typically include four key cues: threat severity, targeted population's susceptibility, recommendation efficacy, and the population's capability to execute the recommendations (Witte, 1992). According to PMT, each cue triggers a specific cognitive mediation process in the targeted group (Milne et al., 2000). While fear appeals have been increasingly employed to influence ISec behaviors, extant research presents inconsistent outcomes regarding their efficacy, and offers limited guidance for crafting effective messages. We note two related observations in ISec fear appeals that are relevant to mental representations, which may provide a cognitive explanation for the mixed findings.

First, while extant ISec fear appeal research generally traces a trajectory from the fear appeal message to individual perceptions and subsequently to intentions or behavior, the intermediary step—from message cues to individuals' mental representations of those cues—remains largely unexplored (Figure 4). As previously stated, mental representation of the fear appeal message affects users' related evaluation and decision-making of it. Therefore, understanding users' mental representations could offer insights into the inconsistent effectiveness of fear appeals and potentially guide the development of more impactful messages. For instance, Wall et al. (2019) demonstrated that specificity in a fear appeal enhances an individual's intention to adopt information security measures, possibly because a detailed message facilitates the construction of a clear and tangible mental representation of the ISec threat, leading to more effective decision-making.

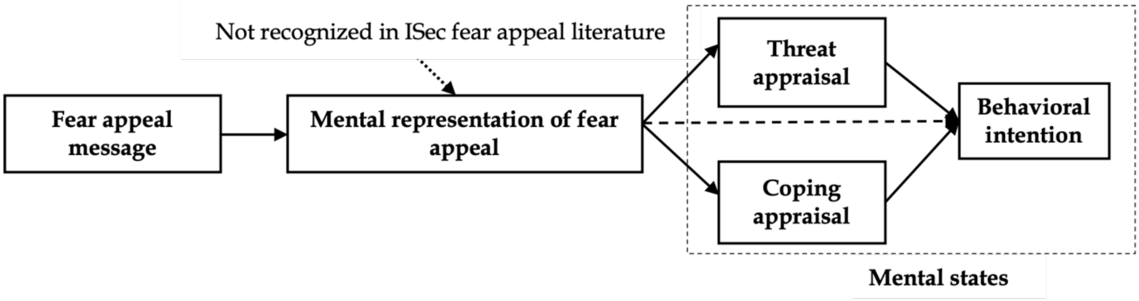


FIGURE 4 Theoretical model and the role of mental representation in fear appeals

The second observation relates to the importance of personal relevance in fear appeals in healthcare field (Maloney et al., 2011; Rogers, 1975; Witte, 1996), which has also recently been highlighted in ISec fear appeals (Boss et al., 2015; Johnston et al., 2015, 2019). However, the concept of "personal relevance" requires two clarifications. The first is regarding threats to oneself versus threats to data/information and the role of personal relevance in both. The second relates to the underlying theory that helps to conceptualize the dimensions of personal relevance. In terms of the former, there is a major difference between fear appeals in healthcare and ISec. Fear appeals in health care study threats of personal relevance directly affect humans (Ruiter et al., 2001, 2014; Williams, 1984). The threat of death from lung cancer, for example, is *direct* on humans.

However, most ISec threats do not directly affect users. They concern information, data, and systems that may or may not have relevance to someone. Even in life-threatening ISec cases, the problem affects the data and information (Figure 5), not humans directly. Ransomware, for example, can make medical records inaccessible, which can contribute to the death of a patient. In this case, the route of causation does not come from direct ransomware threats on humans (Figure 5 – path 1) but from threats to data and information (Figure 5 – path 2) that may have ramifications for users. This fundamental difference is not always clear. Johnston et al. (2015) suggest that "threats to data, information, and systems do not carry the same personal relevance as threats that directly impact one's self, which is common in fear appeal applications in healthcare" (p. 117). They continue that "by overlooking the critical underlying assumption of the threat dimension of fear appeals, researchers have mis-specified the theory within the information security context" (Johnston et al., 2015, p. 117). To account for the importance of personal relevance, Johnston et al. (2015) used sanctioning rhetoric in the fear appeal framework, shifting the threat from data, information, and systems to people themselves. Organizations' sanctions can directly affect users in some cases (Johnston et al., 2015). However, in this case, the threat does not come from ISec but organizational sanctions. The point is that the accounts of personal relevance in ISec threats should consider the data and information and their relevance to the users.

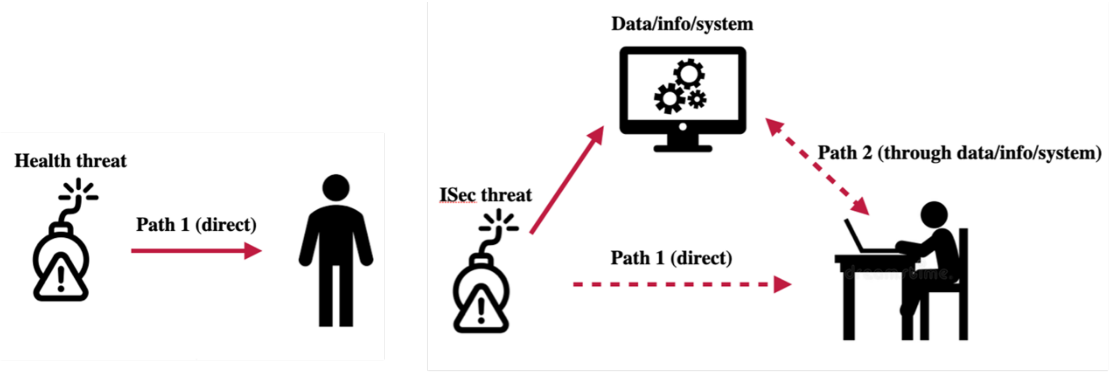


FIGURE 5	Threaten paths of health threat vs. ISec threat

The second clarification of personal relevance relates to its conceptualization regarding threats to information and data. In order to manipulate personal relevance regarding these threats, it is necessary to understand the manipulated dimensions theoretically. This paper contends that psychological distance can make the concept of personal relevance more concrete in both form and degree since both psychological distance and personal relevance use the self as a reference point. For example, when we evaluate how relevant an ISec threat is to ourselves, we may have an image in our minds as to how close or far we are away from the threat. Thus, dimensions of psychological distance can help to measure the extent of personal relevance.

In summary, while the role of mental representation in ISec fear appeals is acknowledged, existing literature lacks a theoretical framework elucidating the causal mechanisms linking fear appeal messages to mental states and subsequently to intentions or behaviors (see Figure 4). Furthermore, prior research underscores the importance of the personal relevance of fear appeals (Johnston et al., 2015, 2019; Maloney et al., 2011; Ruiter et al., 2001, 2014; Witte, 1996). This concept should be extended to encompass threats to data, information, and systems, which are integral to ISec fear appeals. Manipulating such relevance, however, necessitates a well-defined conceptualization of the dimensions involved, for which four dimensions of psychological distance prove instructive.

4.2.4 Previous studies on CLT in information security

While numerous ISec studies address CLT and fear appeals, most remain theoretical and neglect the role of mental representations, as evidenced in Table 8.

TABLE 8 Overview of ISec articles that cite CLT

Study	Context	Theory	Method
Frank & Kohn (2023)	Reveals a dual nature of the extra-role security behaviors in organizations: beneficial and harmful, and explores the motivators behind different types of extra-role security behaviors.	self-determination theory; CLT	semi-structured interview
Schuetz et al. (2020)	Explains how temporal distance and the nature of arguments affect fear appeal assessments based on CLT.	CLT; PMT	Experiment design
Schuetz et al. (2020)	Studies the impact of the message abstractness degree on the outcome of the fear appeal. Results showed that concrete fear appeals are more effective than abstract fear appeals and help stimulate the desired protective response.	CLT; PMT	Experiment design; MANCOVA
Orazi et al. (2019)	Discusses the possibility of introducing CLT as a theoretical lens for designing fear appeals.	CLT; PMT	Review
Lin et al. (2019)	Plans to build a model to understand the effects of information security advocacy.	CLT; PMT; Regulatory Focus Theory	Research plan
Schuetz et al., (2016)	Plans to use CLT to design fear appeal messages, the aim is to explain how brief training in form of a fear appeal can educate users and arouse protective motivation.	CLT; PMT	Research plan

As a further illustration of this, Orazi et al. (2019), a good candidate in terms of the most comprehensive ISec studies discussing CLT and fear appeals, will be examined. They introduced CLT as "a theoretical lens to design and identify potential confounds in fear appeal manipulations" and viewed it as a means of manipulating fear appeals (Orazi et al., 2019, p. 397). They emphasized that the receiver and the message are distinct components in the communication process. Despite this, Orazi et al. (2019) overlooked the role of mental representation in shaping individuals' responses to fear appeals. CLT, a cognitive psychological framework, examines how varying levels of abstraction and psychological distances influence individuals' mental states. Therefore, it is related to fear appeal design but is also vital in understanding the cognitive process through which the receiver represents the message. This study argues that CLT offers crucial theoretical support for ISec research as to what should be manipulated in fear appeals and explains how individuals processing the information (i.e., mental representation) conveyed in fear appeals, which will affect the following mental states in PMT. PMT and CLT can therefore be integrated in this way.

As shown in Table 8, previous ISec studies on CLT overlooks the influence of mental representations and presents conflicting assumptions. For example, Schuetz et al. (2016) argue that a high-level construals of ISec threats heighten threat severity perception, whereas Lin et al. (2019) posit the converse.

4.3 Hypotheses development in Study 2

In this section, we explore the impacts of individuals' construal levels and the psychological distances on individuals’ ISec related threat appraisal and behavioral intentions respectively. Additionally, we discuss the mediating role of threat appraisal in this context.

4.3.1 The impact on individuals’ threat appraisal

Per CLT, an individual's appraisal of ISec threats is mediated by their mental construal level and the psychological distance they perceive to the threat (Mccarthy, 2018; Yaacov Trope & Liberman, 2010). Low-level construals of ISec threats makes them seem more likely to happen to users compared to high-level construals (Liberman, Trope, & Wakslak, 2007). Theoretically, this is attributable to the fact that detailed construals enable the search for confirmatory information, thereby enhancing the perceived likelihood of the threat (M. K. Johnson et al., 1993; Koehler, 1991). Consequently, low-level construals of ISec threats may heighten individuals' perception of threat vulnerability. Previous research suggests that the concrete construals of negative consequences of threats produce a higher threat severity perception by enhancing individuals’ confidence in the reality of negative consequences (Sherman et al., 1985; Wurtele & Maddux, 1987).

Similarly, the framing of threats in terms of psychology distance enhances threat appraisals. For example, framing the negative outcome of the threat as temporal proximal (e.g., every day, suddenly) resulted in individuals perceiving the threat to be more severe than distal temporal framing (e.g., every year) (Chandran & Menon, 2004; Wurtele & Maddux, 1987). According to CLT, this is due to the bidirectional relationship between psychological distance and explanatory level (Liberman, Trope, & Stephan, 2007; Yaacov Trope & Liberman, 2010). ISec has produced related findings, albeit not exclusively grounded in CLT and psychological distance (Johnston et al., 2019; S. W. Schuetz, Benjamin Lowry, et al., 2020; Wall & Warkentin, 2019). Schuetz et al. (2020) showed that fear appeals framed in concrete terms elicited greater perceptions of threat severity and vulnerability than those framed abstractly. Furthermore, Johnston et al. (2019) demonstrate that the efficacy of fear-appeal messages among employees hinges on the congruence between language style and the employees' level of organizational identification. Specifically, those with high organizational identification are more responsive to messages framed from an organizational perspective, such as "our computer systems may be under attack...", leading to heightened threat perception and protection intention (Johnston et al., 2019, p. 281). Conversely, employees with low organizational identification are more responsive to individually framed messages, such as "your computer systems may be under attack...", resulting in greater threat perception (Johnston et al., 2019, p. 280). By matching the personal relevance between organizations and employees, essentially shortening the psychological distance from the threats in organizations, the study increases their threat appraisal to achieve the persuasion goal. Thus, we hypothesize that:

H1 As compared to high-level construals of ISec threats, individual users with low-level construals of ISec threats will perceive a higher (a) threat severity and (b) threat susceptibility.

H2 As compared to the distal psychological distance (including temporal, spatial, social distance, and hypotheticality) of ISec threats, individual users who perceive psychological proximal ISec threats will have a higher (a) threat severity and (a) threat susceptibility perception.

4.3.2 The impacts on the behavioral intentions of individuals

Construal levels and the psychological distance associated with ISec threats also influence individuals' behavioral intentions. Tam et al. (2010) demonstrate that individuals are unconcerned about poor password-management risks if the negative consequences primarily affect others, illustrating the impact of distal social distance. Such individuals often "do not see any immediate negative consequences to themselves" (Ibid, p. 233). Manipulating the onset time of the negative consequences of ISec threats, the temporal distance, may enhance the individuals' ISec protection intentions (Boss et al., 2015; Vance et al., 2013). Wall & Warkentin (2019) also find that detailed, low-level construal fear appeal messages are more effective than general ones in encouraging compliance. While not explicitly framed within CLT, these findings can be theoretically situated within the concepts of psychological distance and construal levels.

Users exhibit heightened motivation to adopt security precautions and enact behavioral changes when ISec threats are perceived as imminent (Murdock & Rajagopal, 2017; Workman et al., 2008). This aligns with CLT, which posits that individuals are less inclined to take immediate action for psychologically distant outcomes due to a perceived lack of control over such events (Yaacov Trope & Liberman, 2003, 2010). Not responding to psychological distal ISec threats on time may be compensated for by coping in the future, while proximal psychological distance ISec threats require immediate responses. Consequently, a greater psychological distance from ISec threats may diminish the urgency for protective responses. Additionally, ISec threats pose risks that necessitate adaptive, risk-mitigating behaviors. According to Kahneman & Lovallo (1993), individuals who perceive risk events as distinct and pay greater attention to their contextual distinctions are more inclined toward risk-aversion. In contrast, those who generalize risks are less risk-averse. It may be another reason why low-level construals and proximal psychological distances in ISec threats tend to elicit compliance with recommended responses. Specifically, perceiving an ISec threat as an isolated event heightens risk-avoidance intentions. Conversely, high-level construals of ISec threats may lead individuals to assimilate these risks into their broader life calculus, rendering them more willing to accept such risks. Therefore, in alignment with CLT and psychological distance considerations, the following hypotheses are posited.

H3 Individual users with low-level construals of ISec threats will more intend to adopt recommended responses than users with high-level construals of ISec threats.

H4 Individual users who perceive psychological proximal ISec threats will more intend to adopt recommended responses than those who perceive ISec threats at a distal psychological distance (including temporal, spatial, social distance, and hypotheticality).

4.3.3 The cognitive mediating role of threat appraisal

The increased intention to take recommended responses is due to individuals' construal level and the psychological distances of ISec threats, and is influenced by individuals' ISec threat appraisal (Rogers, 1983; Rogers et al., 1997). Additionally, as previously mentioned, threat appraisal may be affected by how individuals construct the threat and their perception of psychological distance from the threat. Therefore, this study hypothesizes that:

H5 The effect of the construal level of ISec threats on individuals' intention to adopt recommended responses is mediated by threat appraisal (i.e., threat severity and susceptibility).

H6 The effect of the psychological distance of ISec threats on individuals' intentions to adopt recommended responses is mediated by threat appraisal (i.e., threat severity and susceptibility).

4.4 Research methodology of Study 2

This section outlines the experimental design and methodology in Study 2, including the manipulation check, validation of instruments, and assessment of common method bias. It concludes with an analysis of the results.

4.4.1 Experimental design and procedure in Study 2

A classical experimental design examined how construal levels and psychological distances influenced users' perceptions of mobile malware threats and their protective intentions. The classical experimental design is chosen to, "minimize extraneous variation and increases the likelihood that an experiment will produce valid, consistent results" (Kantowitz et al., 2014, p. 64). Additionally, classical design is typical for research on the effect of fear appeal on behavioral intent (Leventhal, 1970). This study employed a between-subjects design. Participants employed from China were randomly allocated to either experimental or control groups to ensure group equivalence. All groups underwent a pre-treatment survey, received a specific treatment message, and then completed a post-treatment survey. Experimental groups received messages with distinct manipulations (high vs. low) concerning the construal level or psychological distance of the mobile malware threat, whereas the control group received a baseline message. Consistency in measurements was maintained by using identical pre- and post-surveys. Participants progressed sequentially through the study without backtracking or skipping phases. Please check Appendix for more details of experimental treatment messages.

The experimental process focuses on the construal level and three dimensions of psychological distance: temporal, spatial, and hypotheticality, which were successfully manipulated in a pilot test for subsequent experiments. Despite unsuccessful manipulation attempts for the social distance dimension, its impact was assessed through participants' prior experiences with mobile malware threats. This approach is justified by ISec studies suggesting prior experience notably influences user perceptions and intentions (Mwagwabi et al., 2014; Srisawang et al., 2015; Tsai et al., 2016; Zahedi et al., 2015). Participants were queried about such experiences at the questionnaire's conclusion to avoid biasing their experiment responses. Those without relevant ISec threat experiences were excluded from the social distance group.

4.4.2 Data analysis and results of Study 2

Six manipulation check questions were used to assess the efficacy of the fear appeal treatment. Analysis of variance (ANOVA) results verified the intended effects, with significant variations observed in participants' perceptions across experimental groups, indicating their awareness of the manipulations. All constructs in the pretest and posttest of this study passed the reliability and validity check. Upon evaluation, Study 2 exhibited minimal threat of common method bias. Methods of validity, reliability and common method bias checks refer to the methods in Study 1.

A multivariate analysis of covariance (MANCOVA) was employed to assess the influence of psychological distance and construal level on threat appraisal and behavioral intention, with fixed factors set by the manipulation levels of each experimental group and six control variables as covariates. Preconditions for each group were evaluated prior to the MANCOVA, confirming data suitability, and meeting the assumptions of regression homogeneity and variance homogeneity (Alin, 2010; Daoud, 2017; Davis, 2003).

After covariate adjustment, the MANCOVA analysis revealed significant differences in threat appraisal and protection intentions among experimental groups under various treatment conditions, except for the spatial distance group, post-intervention (Table 9). Subsequent post hoc analyses for the social distance group—which had three levels: self, relatives/friends, and strangers—indicated that participants who personally experienced malware threats reported elevated perceptions of threat severity ($p<0.001$), vulnerability ($p<0.005$), and protection intentions ($p<0.005$) compared to those who heard of strangers facing similar threats. Likewise, these subjects perceived greater threat severity ($p<0.05$) and vulnerability ($p<0.05$) than those informed of threats to their relatives, friends, or colleagues. Factors such as low-level threat construal, proximal spatial distance to threatened data, as well as near temporal and social distance to the threat, coupled with high hypotheticality, were observed to heighten subjects' threat perceptions, and bolster their intentions to comply with recommended protective measures. These findings lend empirical support to Hypotheses 1.4, addressing construal level, temporal and spatial distance, social distance, and hypotheticality.

TABLE 9 MANCOVA results - the impact of different levels of psychological distance and construal level on threat appraisal and behavioral intention

<table>
<tr><th rowspan="2">Experimental groups</th><th rowspan="2">Dependent variables</th><th colspan="3">Treatment conditions</th><th colspan="3">MANCOVA results</th></tr>
<tr><th>High-level Mean (SD)</th><th colspan="2">Low-level Mean (SD)</th><th>F</th><th><i>p</i></th><th>Partial η²</th></tr>
<tr><td rowspan="3">Construal level</td><td>Threat severity</td><td>5.22(1.02)</td><td colspan="2">6.06(1.00)</td><td>12.519</td><td>0.001</td><td>0.166</td></tr>
<tr><td>Threat vulnerability</td><td>4.73(1.16)</td><td colspan="2">5.29(1.07)</td><td>4.344</td><td>0.041</td><td>0.065</td></tr>
<tr><td>Protection intention</td><td>4.42(1.48)</td><td colspan="2">5.16(1.22)</td><td>12.254</td><td>0.001</td><td>0.163</td></tr>
<tr><td><b>Experimental groups</b></td><td><b>Dependent variables</b></td><td><b>Proximal Mean (SD)</b></td><td colspan="2"><b>Distal Mean (SD)</b></td><td><b>F</b></td><td><b><i>p</i></b></td><td><b>Partial η²</b></td></tr>
<tr><td rowspan="3">Temporal distance</td><td>Threat severity</td><td>5.23(1.16)</td><td colspan="2">5.95(1.00)</td><td>8.771</td><td>0.004</td><td>0.126</td></tr>
<tr><td>Threat vulnerability</td><td>4.34(1.07)</td><td colspan="2">5.26(1.01)</td><td>16.693</td><td>0.000</td><td>0.215</td></tr>
<tr><td>Protection intention</td><td>4.44(1.34)</td><td colspan="2">5.50(1.02)</td><td>11.654</td><td>0.001</td><td>0.160</td></tr>
<tr><td rowspan="3">Information spatial distance</td><td>Threat severity</td><td>4.53(1.61)</td><td colspan="2">5.87(1.08)</td><td>22.207</td><td>0.000</td><td>0.270</td></tr>
<tr><td>Threat vulnerability</td><td>4.51(1.23)</td><td colspan="2">5.25(1.12)</td><td>8.011</td><td>0.006</td><td>0.118</td></tr>
<tr><td>Protection intention</td><td>4.56(1.12)</td><td colspan="2">5.26(1.03)</td><td>5.319</td><td>0.025</td><td>0.081</td></tr>
<tr><td rowspan="3">Spatial distance</td><td>Threat severity</td><td>5.30(1.32)</td><td colspan="2">5.78(1.24)</td><td>1.679</td><td>0.198</td><td>0.019</td></tr>
<tr><td>Threat vulnerability</td><td>4.82(1.21)</td><td colspan="2">5.14(1.42)</td><td>0.628</td><td>0.430</td><td>0.007</td></tr>
<tr><td>Protection intention</td><td>5.32(1.11)</td><td colspan="2">5.48(1.21)</td><td>0.053</td><td>0.818</td><td>0.001</td></tr>
<tr><td rowspan="3">hypotheticality</td><td>Threat severity</td><td>5.19(1.19)</td><td colspan="2">6.10(0.94)</td><td>9.748</td><td>0.003</td><td>0.148</td></tr>
<tr><td>Threat vulnerability</td><td>4.53(1.33)</td><td colspan="2">5.60(1.27)</td><td>7.973</td><td>0.007</td><td>0.125</td></tr>
<tr><td>Protection intention</td><td>4.30(1.21)</td><td colspan="2">5.19(1.11)</td><td>4.958</td><td>0.030</td><td>0.081</td></tr>
<tr><td><b>Experimental groups</b></td><td><b>Dependent variables</b></td><td><b>Proximal</b></td><td><b>Medium</b></td><td><b>Distal</b></td><td><b>F</b></td><td><b><i>p</i></b></td><td><b>Partial η²</b></td></tr>
<tr><td rowspan="3">Social distance</td><td>Threat severity</td><td>5.87(1.04)</td><td>5.44(1.01)</td><td>5.04(0.93)</td><td>13.819</td><td>0.000</td><td>0.077</td></tr>
<tr><td>Threat vulnerability</td><td>4.96(1.31)</td><td>4.42(1.23)</td><td>4.35(0.93)</td><td>5.619</td><td>0.004</td><td>0.033</td></tr>
<tr><td>Protection intention</td><td>4.49(1.31)</td><td>4.32(1.11)</td><td>3.85(1.06)</td><td>4.291</td><td>0.014</td><td>0.025</td></tr>
</table>

Using bootstrapping techniques, we evaluated the mediation of threat appraisal between construal level/psychological distance, and behavioral intention due to its robust statistical power and non-reliance on normal distribution (Hayes et al., 2011; Preacher et al., 2007; Preacher & Hayes, 2008). The independent variables were construal levels and dimensions of psychological distance, with behavioral intentions as the dependent variable and threat appraisal as the mediator in a serial two-mediator model.

Mediation analyses were performed on five experimental groups, with results depicted in Table10 and Figure 6. In the construal level group, vulnerability fully mediated the relationship between construal level and protection intention, while severity showed no mediation. In the temporal distance group, severity partially mediated the effect of construal level on protection intention. For the spatial distance group, vulnerability fully mediated the impact of temporal distance on protection intention. In the social distance group, both severity and vulnerability were confirmed as full mediators, with a series mediation effect observed between them. The hypotheticality group showed no significant mediation among variables. Overall, these findings provide partial support for hypothesis 5 and 6.

TABLE 10 Summary of mediation effects on different experimental groups

Group	Type	Path	Effect	SE	95% C.I.	
					Lower	Upper
Construal level	Direct	Treatment level → intention	0.349	0.328	-0.304	1.003
		Treatment level→ vulnerability → intention	0.178	0.136	0.0001	0.534
	Indirect	Treatment level→ vulnerability → severity → intention	0.026	0.028	-0.004	0.137
		Treatment level → severity → intention	0.188	0.188	-0.065	0.663
Temporal distance	Direct	Treatment level → intention	0.656	0.250	0.156	1.155
		Treatment level → severity → intention	0.531	0.194	0.199	0.983
	Indirect	Treatment level→ severity → vulnerability → intention	-0.058	0.074	-0.222	0.067
		Treatment level→ vulnerability → intention	-0.075	0.097	-0.327	0.071
Spatial distance for information	Direct	Treatment level → intention	0.447	0.254	0.192	1.205
		Treatment level→ vulnerability → intention	0.278	0.145	0.037	0.621
	Indirect	Treatment level→ vulnerability → severity → intention	-0.008	0.053	-0.145	0.087
		Treatment level → severity → intention	-0.018	0.109	-0.244	0.199
Social distance	Direct	Treatment level → intention	0.160	0.089	-0.015	0.335
		Treatment level→ vulnerability → intention	0.078	0.029	0.033	0.145
	Indirect	Treatment level→ vulnerability → severity → intention	0.017	0.009	0.004	0.042
		Treatment level → severity → intention	0.050	0.024	0.012	0.110
Hypotheticality	Direct	Treatment level → intention	0.523	0.303	-0.083	1.128
		Treatment level→ vulnerability → intention	0.233	0.212	-0.098	0.750
Hypotheticality	Indirect	Treatment level→ vulnerability → severity → intention	0.075	0.111	-0.110	0.338
		Treatment level → severity → intention	0.060	0.112	-0.079	0.426

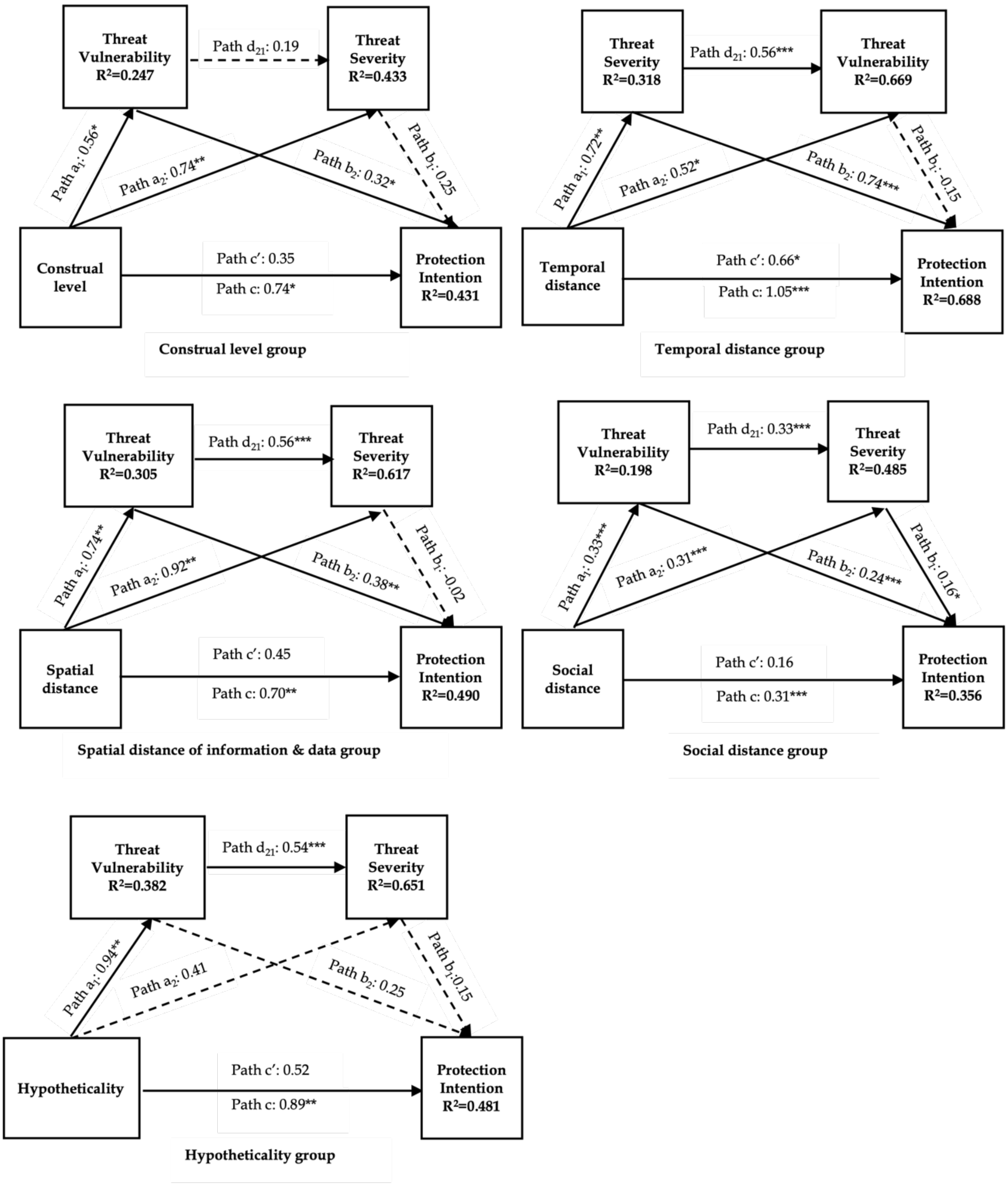


FIGURE 6 Multiple mediation model results of Study 2

4.5 Discussion of Study 2

Study 2 evaluates how specific features of threats and individuals' psychological proximity to these threats affect their threat appraisal and protective intentions, revealing that detailed fear appeals and perceived closeness to threats can enhance the persuasiveness of cybersecurity messages. More details of the research results and contributions will be discussed in this section.

4.5.1 Key findings in Study 2

The effective crafting of fear appeal messages is a critical consideration in ISec behavioral research. Although cognitive psychology posits that individuals process these appeals through mental representations, this concept remains underexplored in ISec literature. Such mental schemas, termed "mental representations", influence variables like threat appraisal (Pitt, 2000; Von Eckardt, 2012). Study 2 employs CLT to analyze the mental representations associated with fear appeals.

CLT posits that individuals engage with ISec threats at varying levels of mental abstraction, or 'construal levels.' These levels are influenced by the threat-specific information in the fear appeal and by individuals' subjective psychological distance to the threat. To empirically investigate this, the study conducted experiments that:

1. Varied the construal level of mobile malware threats in fear appeals by manipulating their descriptive features (primary vs. secondary).
2. Adjusted participants' psychological distance to the threat by altering its onset times, locations, and probabilities, as well as participants' familiarity with the jeopardized information.
3. Collected self-reports to assess the social dimension of psychological distance to the threat, asking participants to recount prior experiences with similar threats.

The impact of construal levels and psychological distances on threat appraisal and behavioral intentions in response to fear appeal messages were then examined. Specifically, participants with low-level construals and proximal psychological distances perceived greater threat severity and vulnerability and exhibited higher willingness to comply with recommended actions, compared to their counterparts with high-level construals and distal psychological distances. Notably, this pattern did not hold for the subgroup examining spatial distance. These results suggest that manipulations of mental construal and psychological distance in fear appeals significantly influence individuals' threat assessments and compliance intentions. Therefore, strategically crafting fear appeals to alter these perceptual factors can enhance their persuasive efficacy. No significant differences were observed in threat appraisal and intentions across users with varying perceptions of spatial distance related to mobile malware threats. This is likely because ISec threats, inherently capable of remote attacks, are not geographically constrained like physical threats. Consequently, the geographic origin of an ISec threat does not influence one's spatial distance perception. It may be more effective to manipulate perception through relative physical and virtual proximities, such as comparing the threat to one's own home or organization versus external entities, or one's personal devices versus others (Jaeger et al., 2017).

In accordance with PMT assumptions (Milne et al., 2000; Rogers, 1983), mediation effects were separately assessed across experimental groups to explore the nexus between users' construal levels and psychological distances of ISec threats, their threat appraisal, and behavioral intentions. Except for the hypotheticality group, threat appraisal either fully or partially mediated the relationship between construal levels/psychological distance and behavioral intentions across groups. Notably, these mediation outcomes were inconsistent. Several factors account for this inconsistency. Small variations in sample demographics could contribute to the divergent results, while a reduced sample size in some groups might elevate the likelihood of Type II error, thus undermining the study's statistical power (Freiman et al., 2019). However, higher sample size does help increase the significance level of the findings since the larger the size, the more accurately the entire group's behavior can be reflected (D. H. Johnson, 1999; Lantz, 2013). This claim is corroborated by the social distance group, which exhibited full mediation of threat appraisal between social distance and behavioral intentions due to its sufficient sample size. Therefore, individuals' intentions to comply with recommended actions are at least partially contingent on their threat evaluations.

4.5.2 Contributions to research in Study 2

Study 2 advances the field of fear appeal in information security (ISec) through several key contributions. Foremost, it is the inaugural study to emphasize the critical role of mental representation in shaping individual responses to fear appeals. This focus is essential for two primary reasons. First, cognitive psychology posits that mental representation is the initial cognitive step in processing a fear appeal, especially for intangible or unrealized ISec threats that rely on psychological recognition. Second, an individual's cognitive state toward a fear appeal is contingent on their mental representation, serving as a basis for intentional states like threat evaluations and intentions (Sterelny, 1990; Von Eckardt, 2012). Leveraging CLT to interpret these mental representations, this research engineered fear appeal messages to manipulate individuals' abstraction levels and perceived psychological distance from threats. The results corroborate the efficacy and viability of the approach, revealing distinct cognitive states among individuals based on varying abstraction levels of mental representation.

Second, Study 2 substantiates the utility of CLT as a theoretical framework for designing fear appeals in ISec research, particularly for threat manipulation. The theoretical basis was usually absent in manipulating threats in some previous fear appeal ISec literature. For example, Boss et al. (Boss et al., 2015) manipulated the threat’s onset time in the fear appeal but did not offer any theoretical justifications for their manipulation of onset time. The current study introduces CLT and mental representation as explanatory mechanisms. Specifically, CLT and the four dimensions of psychological distance provide a theoretical underpinning for the persuasiveness of fear appeals. For instance, modifying aspects of the ISec threat—such as onset time, likelihood, and impact—can influence individuals' construal levels and perceptions of psychological distance. These, in turn, affect threat appraisal and behavioral intentions, thereby enhancing the persuasive efficacy of fear appeals.

The third contribution pertains to the integration of CLT concept of psychological distance as a framework for understanding and operationalizing 'personal relevance' in the context of ISec fear appeals. While extant literature (Boss et al., 2015; Johnston et al., 2015; Warkentin et al., 2016) posits the importance of personal relevance for effective fear appeals, the concept remains nebulous and difficult to measure systematically. Psychological distance offers a delicate approach for conceptualizing personal relevance, as both involve self-referential thinking to assess the 'distance' between oneself and the ISec threat. If the psychological distance is used to understand personal relevance, its cognitive mechanism, which affects individuals' mental states, can be interpreted from a CLT-based perspective. That is, the personal relevance of the threat (namely psychological distance) may affect the threat appraisal and subsequent intention by changing individuals' construal level of the threat. Furthermore, leveraging psychological distance enables the precise manipulation of personal relevance across its four dimensions—temporal, spatial, social, and hypotheticality—thereby offering a methodological advance in fear appeal design. Unlike health-related appeals, ISec appeals target threats to information, data, or systems rather than individuals directly. This study demonstrates that modulating construal levels and dimensions of psychological distance can sharpen the focus of personal relevance to these targeted assets, thereby enhancing threat appraisal and behavioral intent.

Finally, Study 2 reveals that mental construal and psychological distance shape behavioral intentions, at least in part, through the mechanism of threat appraisal. PMT believes that threat appraisal plays a cognitive mediation role between the fear appeal message and individuals’ protection intention (Rogers, 1983; Rogers et al., 1997). In the context of cognitive psychology, individuals evaluate threats based on their mental schemas (Sternberg & Sternberg, 2011). By integrating cognitive psychology with PMT, this study enriches our understanding of the cognitive pathways underlying fear appeal processing. Specifically, individuals' mental representations of threats influence their behavioral intentions, and this influence is at least partially mediated by threat appraisal—a topic not explored in extant CLT-related ISec fear appeal literature (Y.-Y. Lin et al., 2019; Mady & Gupta, 2017; Orazi et al., 2019; S. Schuetz et al., 2016; S. W. Schuetz, Benjamin Lowry, et al., 2020; S. W. Schuetz, Lowry, et al., 2020).

4.5.3 Implications of Study 2 for practice

The study's findings yield several actionable recommendations for ISec practitioners leveraging fear appeal communications in Security Education, Training, and Awareness (SETA) initiatives:

4. Enhanced Specificity. Instead of employing abstract fear appeals, provide detailed descriptions of ISec threats. Specificity, such as outlining the sequence of events following a threat, helps lower an individual's construal level (Jenkins et al., 2014).
5. Inclusion of Secondary Features. While emphasizing primary characteristics like the harmful nature of the ISec threat is crucial, augment this with secondary features. For instance, explain how mobile spyware comes bundled with benign software and silently collects data.
6. Psychological Distance Manipulation. To increase personal relevance and impact construal levels, use language and scenarios that narrow the psychological distance. Employ first-person perspectives and describe imminent or highly probable threats.
7. Persuasive Enhancement through Relevance. Increase the fear appeal's effectiveness by making the individual feel responsible for or connected to the threatened data. This can be achieved by stressing the data's familiarity or importance.

Further, drawing on Kumaraguru et al. (2010), incorporating graphical elements in ISec training materials can facilitate lower-level construals. CLT indicates that it is because the graphics' information is more intuitive and detailed, which helps individuals generate low-level construal regarding the object (Yaacov Trope & Liberman, 2010). Similarly, emphasizing social consequences over health impacts in fear appeals can heighten perceived urgency and vulnerability (Murdock & Rajagopal, 2017). Future ISec fear appeal strategies could benefit from these insights.

4.5.4 Limitations of Study 2 and future research

Study 2 has limitations related to scope and applicability. First, it exclusively focuses on the threat element within fear appeals, neglecting the recommendation component. This leaves unresolved questions about how individuals cognitively process recommendations in fear appeals and its impact on mental states like self-efficacy. Incorporating CLT to study the recommendation component could enhance the methodological rigor of ISec fear appeal research, as prior works have shown that detailing countermeasures in appeals improves persuasiveness (Johnston et al., 2015; S. W. Schuetz, Benjamin Lowry, et al., 2020). Future research should address the diverse mental construals individuals might employ regarding recommendations, and their influence on mental states. Second, while focusing on individual users offers insights into CLT's application to personal ISec contexts, the findings have limited generalizability to organizational settings (Aurigemma & Mattson, 2019). Organizational users interact with fear appeals under different conditions—such as policy constraints and organizational identification—which may affect their cognitive processes differently. Innovative CLT-based designs targeting organizational contexts can offer unique insights; for example, aligning fear appeal language with employees' organizational identification has proven effective (Johnston et al., 2019).

4.6 Conclusions from Study 2

This paper advances the understudied field of Information Security (ISec) fear appeals by examining the pivotal role of mental representations based on cognitive psychology. It posits that users form initial mental representations of a fear appeal, which significantly influence subsequent cognitive evaluations and behaviors. Employing Construal Level Theory (CLT), the study integrates mental construal and psychological distance into the design of ISec fear appeals. Results indicate that these elements substantially affect threat appraisal and the intention to comply with recommended actions. Specifically, fear appeals that foster low-level construal and proximal psychological perceptions of ISec threats are more effective. This research not only elucidates the cognitive mechanisms underlying the processing of fear appeals but also offers new insights into the design of persuasive ISec messages.

5 STUDY 3: UNDERSTANDING THE INWARD EMOTION-FOCUSED COPING STRATEGIES OF INDIVIDUAL USERS IN RESPONSE TO MOBILE MALWARE THREATS

This study explores how individuals cope with ISec threats through EFC strategies, highlighting the lack of understanding and potential confusion around EFC in information security. It empirically assesses five inward EFC strategies within the mobile malware context, contributing new findings on EFC's impact on protective intention and differentiating between active and passive EFC forms, thereby offering insights for information security research and practice.

5.1 Introduction to Study 3

In the ISec field, coping theory categorizes two key coping mechanisms: Problem-Focused Coping (PFC) and Emotion-Focused Coping (EFC). PFC involves actions that directly address threats, such as installing anti-malware software. In contrast, EFC, often linked to risk-taking behaviors, includes strategies that aim to reduce emotional distress rather than directly tackling the threat, like ignoring anti-malware recommendations (Lazarus & Folkman, 1984; Liang et al., 2019; Liang & Xue, 2009). EFC can be further divided into inward and outward strategies, with the former often leading to risky information practices due to the suppression of negative emotions and altered perceptions of ISec threats (Liang et al., 2019).

There is a gap in understanding the various inward EFC strategies and their impact on ISec behaviors. For instance, the distinctions between EFC and PFC have sometimes been blurred in past research. To address this, a study was conducted to evaluate different inward EFC strategies, aiming to clarify their effects on ISec practices and contribute to the body of knowledge in ISec behavior.

This research helps in identifying how various cognitive factors influence the adoption of these strategies, providing valuable insights for ISec education and further studies focusing on EFC in ISec.

5.2 Research methodology and result of Study 3

Our study successfully utilized the maximum likelihood method for structural equation modeling, with all fit indices aligning with the standards established by Hooper, Coughlan, and Mullen (2008). It confirmed the model's effectiveness. Our optimal model explained various degrees of variance in inward EFC responses: 8% in avoidance, 16% in reactance, 30% in hopelessness, 7% each in fatalism and wishful thinking, and 40% in protection intention. The R-squared values for endogenous variables were significant, showcasing the model's explanatory capability.

The analysis revealed that response efficiency and self-efficacy positively influenced users' protection intention, partially supporting our hypotheses. Interestingly, threat vulnerability positively influenced fatalism and hopelessness while slightly decreasing wishful thinking, yet it didn't significantly impact reactance and avoidance. Response efficacy negatively affected several inward EFC strategies, including avoidance and fatalism, which in turn negatively influenced protection intention. However, reactance, wishful thinking, and hopelessness showed no significant impact on protection intention. Contrary to expectations, perceived threat severity did not positively affect inward EFC strategies but negatively impacted avoidance, reactance, and hopelessness. Additionally, self-efficacy didn't significantly affect any inward EFC strategy (please see Table 11 and Figure 7 for more details).

TABLE 11 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
H5a: 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⩽0.05, **p⩽0.01, ***p⩽0.001, † 0.05⩽p⩽0.1, n/s refers to insignificant

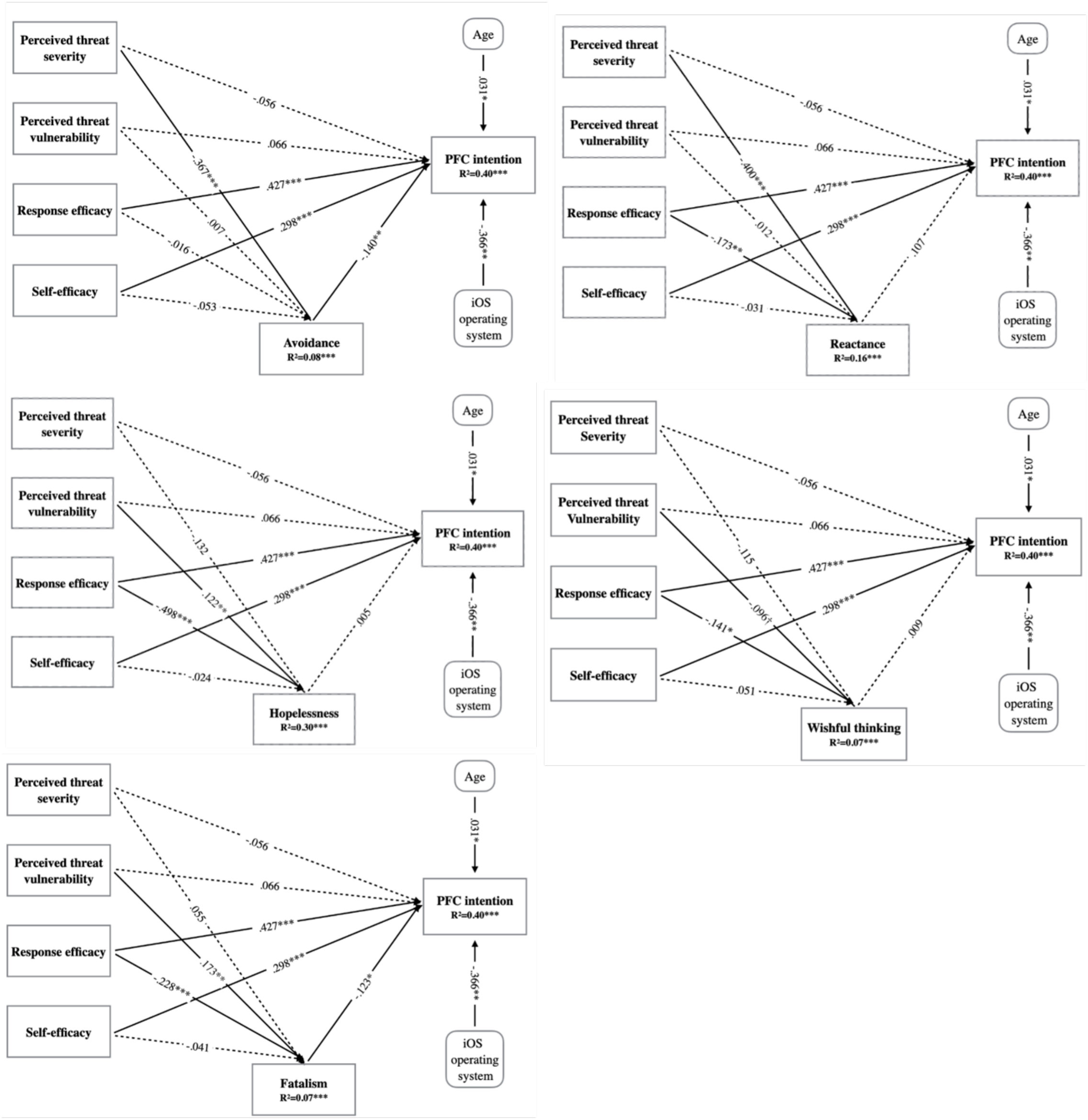


FIGURE 7 Model test results of Study 3

5.3 Discussion of Study 3

5.3.1 Key findings in Study 3

The study examined how different inward EFC strategies influence users' PFC response to mobile malware threats, considering the role of cognitive factors. It found that avoidance and fatalism, considered passive EFC strategies, hinder users' proactive responses, a finding consistent with PMT and previous health psychology research (Carver et al., 1989; Livneh, 2000; Rippetoe & Rogers, 1987). In contrast, when users believe in effective countermeasures against malware, they are more likely to adopt PFC response. The study also explored the influence of perceived threat vulnerability, showing that it increases the likelihood of adopting passive EFC strategies like hopelessness and fatalism, particularly when users view the threat as inevitable. Active EFC strategies, such as avoidance, reactance, and wishful thinking, involve ignoring or distorting facts and are less influenced by perceived threat vulnerability.

Additionally, the study found that users' perception of the severity of mobile malware threats negatively impacts their willingness to adopt certain EFC strategies. Contextual factors, such as familiarity with smartphones and repeated exposure to malware threats, might lead users to underestimate these threats and thus opt for less demanding inward EFC strategies. The study also noted that factors like self-efficacy and individual differences might affect the relationship between EFC strategies and responses to ISec threats, underscoring the complexity of inward EFC responses in the context of malware threats and the need for further research in this area.

5.3.2 Contributions to research and practice in Study 3

Study 3 significantly contributes to ISec behavior research by focusing on individual EFC strategies. Firstly, it reintegrates EFC into the PMT framework, addressing the gap in existing PMT-based security behavior research that primarily emphasizes PFC while overlooking EFC. This study categorizes and clarifies five specific inward EFC strategies, enhancing understanding of how these strategies impede PFC. Secondly, it distinguishes between active and passive inward EFC strategies based on how users perceive and respond to ISec threats. Active strategies involve ignoring or distorting threat perceptions, while passive strategies reflect a negative attitude towards the inevitability of threats. This classification, supported by empirical evidence, adds depth to the ISec literature. Lastly, the study challenges existing hypotheses about ISec behavior, revealing a complex relationship between threat appraisal and EFC strategies. It suggests that contextual factors play a significant role in shaping individual coping responses, urging future research to reevaluate the connection between threat perceptions and EFC responses in ISec.

From the perspective of practical implications, Study 3 points out a gap in the ISec literature regarding the limited exploration of EFC strategies and their cognitive processes, underscoring the need for more comprehensive information behavior education and EFC training. The research found that individual users often underestimate mobile malware threats, leading to inappropriate EFC responses like unrealistic optimism or fatalism. This lack of awareness can hinder effective ISec actions. Therefore, it's crucial for organizations and ISec educators to help users accurately recognize and appropriately respond to these threats. The study suggests that educating users about the severity of mobile malware consequences and providing effective countermeasures can reduce tendencies toward avoidance and fatalism. It emphasizes the need for practical and feasible advice on mobile ISec behaviors and a balanced communication approach to ensure users do not perceive threat consequences as inevitable, providing valuable insights for employee training in mobile phone information security.

5.4 Conclusions from Study 3

The study specifically examines five inward EFC strategies in relation to mobile malware, finding that response efficacy notably reduces the inclination towards reactance, fatalism, wishful thinking, and hopelessness. Additionally, the perception of vulnerability positively influences the adoption of passive EFC strategies. Among these, avoidance and fatalism are particularly detrimental, significantly reducing users' intentions to proactively protect their mobile ISec.

6 CONCLUSION

In this dissertation, I explore prior experience, observational learning, and inward emotion-focused coping in PMT, introducing the concept of mental representation in fear appeal message design. They are core components of PMT that are ignored in ISec environments. Through an in-depth exploration of these components, this research could make some contributions to correcting the one-sided or distorted view of individual motivations and behaviors that may arise when PMT is applied to information security.

The dissertation is structured into three studies. Study 1 offers a detailed perspective on ISec-related prior experience, which proposes a comprehensive perspective that encompasses the entirety of an individual's encounter with an ISec incident— from occurrence to resolution and incorporated vicarious experiences (or observational learning) into the content framework of PE. It enriches the conceptualization of prior ISec experience and constitutes a novel contribution to the field of ISec in particular by exploring prior coping feedback. Study 2 melds concepts of mental construal and psychological distance from CLT to craft ISec fear appeals, elucidating the potential of leveraging individuals' mental representation tendencies to shape threat appraisals and protective intentions effectively. Study 3 distinctly identifies and empirically tests five inward EFC strategies, and further differentiates them into positive and negative modes. During the research, some interesting triggers and nuances in behavior behind individuals' ISec behaviors were identified. For example, cognitive biases such as unrealistic optimism, and varied rationales behind similar maladaptive coping behaviors.

In conclusion, this dissertation significantly bridges existing knowledge gaps, offering both researchers and practitioners a more holistic insight into motivations and behaviors in the ISec context. The findings pave the way for the development of enhanced strategies and solutions, fostering a more balanced and comprehensive understanding of the application of PMT in information security.

YHTEENVETO (SUMMARY IN FINNISH)

Tässä väitöskirjassa tutkitaan suojamotivaatioteoriassa aikaisempaa kokemusta, havainnoivaa oppimista ja sisäänpäin suuntautuvaa emotionaalista selviytymistä ja esitellään mentaalisen representaation käsite pelottelevien viestien suunnittelussa. Ne ovat suojamotivaatioteorian ydinkomponentteja, jotka jätetään huomiotta tietoturvaympäristöissä. Syvällisen tutkimuksen kautta tämä tutkimus voisi korjata yksipuolista tai vääristynyttä näkemystä yksilöiden motivaatioista ja käyttäytymisestä, joka voi ilmetä, kun suojamotivaatioteoriaa sovelletaan tietoturvaan.

Väitöskirja on jaettu kolmeen tutkimukseen. Tutkimus 1 tarjoaa monipuolisen näkemyksen aikaisemmasta tietoturvakokemuksesta. Tutkimus ehdottaa kokonaisvaltaista näkökulmaa, joka kattaa yksilön koko tietoturvaloukkauksen kohtaamisen – alkaen tapahtumasta ja päättyen ratkaisuun, ja sisällyttää havainnoivan oppimisen aikaisemman kokemuksen sisältökehykseen. Se rikastuttaa tietoturvakokemuksen käsitteellistämistä ja tuo uuden panoksen tietoturva-alalle erityisesti tutkittaessa aikaisempaa selviytymispalautetta. Tutkimus 2 yhdistää mentaalisen konstruoinnin ja psykologisen etäisyyden käsitteet konstruktiotason teoriasta tutkiakseen, yksilöiden mentaalisen representaation taipumusten mahdollisuuksia muokata uhka-arvioita ja suojautumisaikomuksia tehokkaasti pelottelevia viestejä saatuaan. Tutkimus 3 tunnistaa erikseen ja testaa empiirisesti viisi sisäänpäin suuntautuvaa tunteisiin keskittyvää selviytymisstrategiaa, ja erittelee niitä edelleen positiivisiin ja negatiivisiin muotoihin. Tutkimuksen aikana tunnistettiin mielenkiintoisia laukaisijoita ja vivahteita yksilöiden tietoturvakäyttäytymisen takana. Niistä mainittakoon kognitiiviset vinoumat kuten epärealistinen optimismi ja samankaltaisten sopeutumattomien selviytymiskäyttäytymisten taustalla olevat vaihtelevat perustelut.

Yhteenvetona tämä väitöskirja kuroo umpeen merkittävästi olemassa olevia tietämysaukkoja tarjoten tutkijoille ja ammattilaisille monipuolisemman ja kokonaisvaltaisemman näkemyksen motivaatioista ja käyttäytymisestä tietoturvan yhteydessä. Löydökset tasoittavat tietä kehittyneempien strategioiden ja ratkaisujen kehittämiselle edistäen tasapainoisempaa ja kattavampaa ymmärrystä suojamotivaatioteorian soveltamisesta tietoturvassa.

APPENDIX: THE RESEARCH INSTRUMENTS

Survey items of Study 1:

Threat severity (Adapted from Milne et al., 2002; Witte, 1996)

Sev1: If my mobile phone is infected with malware, it would be severe.

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.

Sev4: If my mobile phone is infected with malicious applications, it would be serious.

Threat vulnerability (Adapted from Witte, 1996)

Vul1: My mobile phone is at risk for becoming infected by malware.

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 programs.

Vul4: There is a chance that harmful software may infect my mobile phone.

Response efficacy (Adapted from Milne et al., 2002; Witte, 1996)

Res1: Updating mobile operating system is effective for preventing my phone from being infected with malware.

Res2: When updating mobile operating system timely, a mobile phone is more likely to be protected.

Res3: If I were to update the mobile operating system timely, the chances of my phone being infected with malware will be lessened.

Res4: If I were to update the mobile operating system timely, I would lessen the chances of mobile malware infection.

Self-efficacy (Adapted from Milne et al., 2002; Witte, 1996)

Self1: Updating mobile operating system timely would be easy for me.

Self2: It would not be difficult for me to update the mobile operating system timely.

Self3: I can update the mobile operating system timely without much effort.

Self4: I feel confident in my ability to update mobile operating system timely.

ISec protective intention (Adapted from Venkatesh et al., 2003)

Int1: I intend to update my mobile operating system timely in the future.

Int2: I predict I will update my mobile operating system timely in the future.

Int3: I plan to update my mobile operating system in a timely manner in the future.

Similarity of the threat (Adapted from Chai et al., 2009; Liang & Xue, 2010; Zahedi et al., 2015)

Sim1: I have suffered from a similar information security threat as mobile malware in the past.

Sim2: I have ever had a similar information security threat when using a mobile phone in the past.

Sim3: The number of similar information security threats I have encountered in the past has been (very low/very high).

Severity of previously experienced ISec threats (direct) (Adapted from Witte, K.,1996; Milne et al. 2002)

P_sev1: My mobile phone was infected by malware before, which caused me major problems.

P_sev2: I was in serious trouble because my mobile phone was infected with malware.

P_sev3: I have suffered a serious consequence due to the mobile malware infection.

Frequency of previously experienced ISec threats (direct) (Adapted from Witte, K.,1996; Milne et al. 2002)

P_fre1: My phone was often infected with mobile malware in the past.

P_fre2: My mobile phone was infected with malware frequently in the past.

P_fre3: The number of times my phone has been infected with malware before is (very low... very high).

Prior Coping behavior (direct)

What have you done after experiencing the incident of the mobile malware infection? (Multiple choice question)

A) I installed the mobile anti-malware for scanning and removing malware.

B) I updated the applications on my phone in time.

C) I took a negative coping behavior (e.g., ignore the malware, restart the phone, etc.).

D) I often update my phone's operating system.

E) I took other positive coping behaviors (e.g., download the mobile software cautiously).

F) I am still the same as before and have not taken any coping behaviors.

Feedback of the prior coping behavior (direct)

After I took such a coping behaviour, I think that,

P_feed1: My mobile phone was effectively protected by this coping behaviour.

P_feed2: This coping behaviour is a good way to protect my phone from malware infection.

P_feed3: This coping behaviour can protect my mobile phone effectively.

Prior vicarious experience items are modified based on the items of prior direct experience.

Items that differentiate between direct and indirect prior experience

Symptoms that your phone was once infected with malware.

- Data usage spikes: data is consumed rapidly for unknown reasons.
- Strange behavior: your phone behaves in unusual ways, such as opening and closing apps by itself, sending text messages, or making phone calls without your permission, or displaying strange error messages.
- Pop-up ads: seeing pop-up ads on your phone's screen, even when you're not using any apps.
- Slow performance: your phone is suddenly running much slower than usual, to the extent that restarting it may not resolve the issue.
- Unauthorized downloading of apps: Unwanted apps, games, porn apps, malware etc. are installed in the background of the mobile phone without

your consent. The installed app cannot be uninstalled or can automatically be reinstalled after uninstalling.

- Property loss: the phone bill is lost for unknown reasons.
- Strange messages: you have received messages with malicious web links or malicious expense deductions.
- Unusual battery drains: your phone's battery to drain much more quickly than usual.

1) According to the above symptoms, have you ever experienced the same or similar mobile malware infection before?

A) Yes, I have the same or similar experience as above.

B) No, I do not have such experience. (Skip to 2)

C) I could not remember.

2) Have you ever heard about mobile malware accident from other ways?

A) My family member's/friend's/classmate's/colleague's mobile phone was once infected with malware.

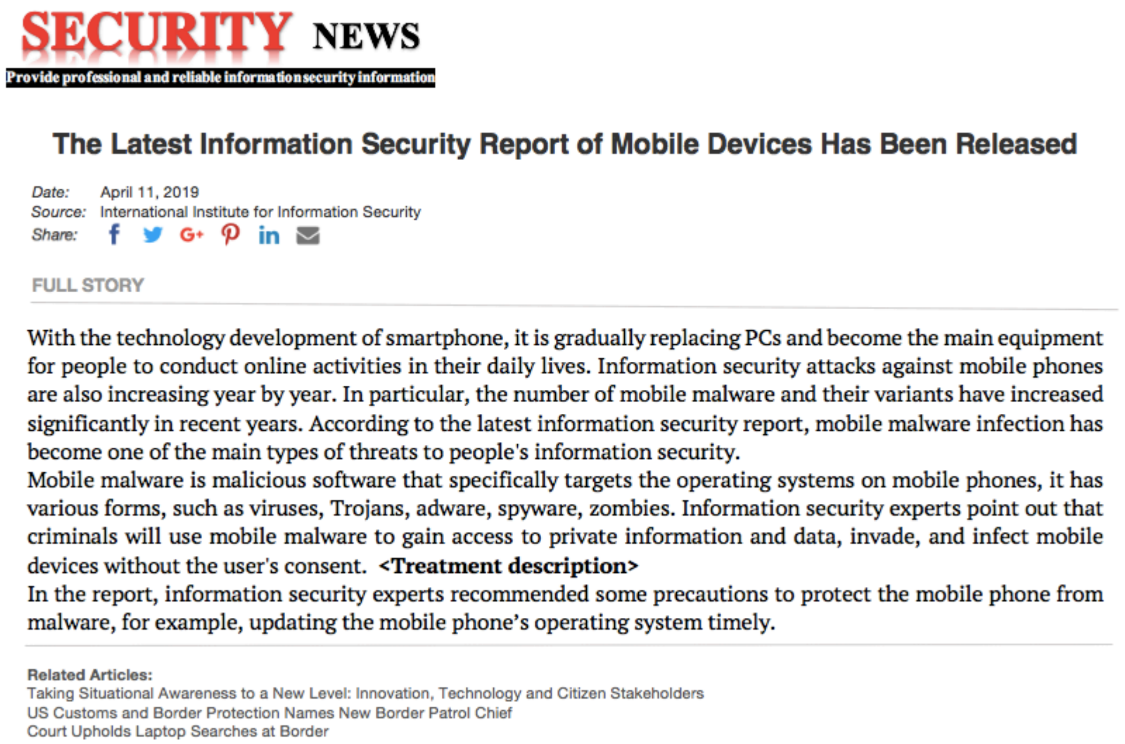
B) I know from other sources that some people's mobile phones were once infected with malware.

C) No, I have never heard of the fact that the mobile phone will be infected with malware.

D) I could not remember.

Survey items of Study 2:

Items of threat severity, threat vulnerability, response efficacy, self-efficacy and protection intention are same as Study 1. Figure 8 shows the baseline message of the experiment in Study 2. The details of manipulation messages are in Table 12.



SECURITY NEWS

Provide professional and reliable information security information

The Latest Information Security Report of Mobile Devices Has Been Released

Date: April 11, 2019

Source: International Institute for Information Security

Share:

FULL STORY

With the technology development of smartphone, it is gradually replacing PCs and become the main equipment for people to conduct online activities in their daily lives. Information security attacks against mobile phones are also increasing year by year. In particular, the number of mobile malware and their variants have increased significantly in recent years. According to the latest information security report, mobile malware infection has become one of the main types of threats to people's information security.

Mobile malware is malicious software that specifically targets the operating systems on mobile phones, it has various forms, such as viruses, Trojans, adware, spyware, zombies. Information security experts point out that criminals will use mobile malware to gain access to private information and data, invade, and infect mobile devices without the user's consent. **<Treatment description>**

In the report, information security experts recommended some precautions to protect the mobile phone from malware, for example, updating the mobile phone's operating system timely.

Related Articles:

Taking Situational Awareness to a New Level: Innovation, Technology and Citizen Stakeholders

US Customs and Border Protection Names New Border Patrol Chief

Court Upholds Laptop Searches at Border

FIGURE 8 Baseline message in Study 2

TABLE 12 Manipulations of the treatment messages in Study 2

Dimensions	**Level**	**Treatment**
Visibility (construal level)	Concrete (low-construal level)	Mobile malware poses threats to mobile phone users' information and data through fake emails, Internet spread, and disguised as legal files. The phone infected with malware can be lagging, the speed of the phone and networking will be significantly slower. Some malwares can always pop-up windows or push ads on the phone screen, cause the phone to crash frequently. Criminals can even use the mobile user's information to steal his/her money by transfers, online consumption, or commit illegal acts by using the mobile user's identity. (With pics)
	Abstract (high-construal level)	The consequences of mobile malware are serious. It can cause the leakage of private information and data of mobile phone users, and even property loss and damage to their reputation. Not only that, but users' mobile malware can also threaten the information security of the environment around them.
Temporal Distance	Distal	The severe consequences of mobile malware infection usually not appearing until after a long time in the future. It is because the attacker uses the time delay to let the application download and start the malicious code after a long period of time to avoid the tracking of the protection system.
	Proximal	The severe consequences of mobile malware infection are usually appearing immediately. It means that once the phone is attacked by malware, in the next second, the malicious

Dimensions	Level	Treatment
		code of the software will be downloaded and launched, and the phone will be monitored and attacked immediately.
Spatial distance (to information)	Distal	The information in the users' mobile phone accessed, damaged, or erased by most mobile malware is images and files downloaded on the web, web browsing records, text messages, seldom used account information, etc. Criminals can use users' identity information to invade the information, data, or system of their school, company, or other organizations.
	Proximal	The information in the users' mobile phone accessed, damaged, or erased by most mobile malware is photos and files of great significance to users, personally identifiable information, important emails, frequently used account information, etc. Criminals can use users' identity information to invade the information, data, or system on their computers.
Spatial distance (to ISec threat)	Distal	However, due to various factors, the locations of users who have been attacked by mobile malware are unevenly distributed. According to the survey, the vast majority of respondents who have experienced mobile malware infection on mobile phones are from China. In particular, mobile malware incidents in central and southern China occurred more frequently.
	Proximal	However, due to various factors, the locations of users who have been attacked by mobile malware are unevenly distributed. According to the survey, the vast majority of respondents who have experienced mobile malware infection on mobile phones are from North America. In particular, mobile malware incidents in the United States occurred more frequently.
Hypotheticality	High hypotheticality	Moreover, mobile malware infection has become the most information security threat with the highest probability of occurrence. According to statistics, in the world, nearly 8 out of every 10 mobile phones have been infected with malware, and 87.9% of mobile phone users have been monitored by malicious applications. Mobile phone users who lost their phone bills due to phishing text messages sending from malware accounted for 61.7%.
	Low hypotheticality	However, the occurrence probability of the mobile malware infection event is lower compared to other information security threats. According to statistics, less than 1 out of every 10 mobile phones in the world have been infected with malware, and only 7.6% of mobile phone users have been monitored by malicious applications. Mobile phone users who lost their phone bills due to phishing text messages sending from malware accounted for only 0.2%.

Survey items of Study 3: Please check the details from the paper of Xin et al. (2022).

REFERENCES

2023 Data Breach Investigations Report. (2023). *Verizon*.

Achterkamp, R., Hermens, H. J., & Vollenbroek-Hutten, M. M. R. (2016). The influence of vicarious experience provided through mobile technology on self-efficacy when learning new tasks. *Computers in Human Behavior*, *62*, 327–332. https://doi.org/10.1016/j.chb.2016.04.006

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11–39). Springer.

Ajzen, I. (1987). Attitudes, traits and actions: dispositional prediction of behaviour in social pshychology. *Advances in Experimental Social Psychology*, *20*, 63.

Ajzen, I. (2002). Residual effects of past on later behavior: Habituation and reasoned action perspectives. *Personality and Social Psychology Review*, *6*(2), 107–122.

Albarracin, D., & Wyer Jr, R. S. (2000). The cognitive impact of past behavior: influences on beliefs, attitudes, and future behavioral decisions. *Journal of Personality and Social Psychology*, *79*(1), 5.

Alin, A. (2010). Multicollinearity. *Wiley Interdisciplinary Reviews: Computational Statistics*, *2*(3), 370–374.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Ashford, S. (2010). What is the best way to change self‐efficacy to promote lifestyle and recreational physical activity? *British Journal of Health Psychology*, *15*(2), 265–288. http://onlinelibrary.wiley.com/doi/10.1348/135910709X461752/full

Atance, C. M., & O'Neill, D. K. (2005). The emergence of episodic future thinking in humans. *Learning and Motivation*, *36*(2 SPEC. ISS.), 126–144. https://doi.org/10.1016/j.lmot.2005.02.003

Aurigemma, S., & Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. *Journal of the Association for Information Systems*, *20*(12), 7.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191.

Bar, M. (2011). *Predictions in the brain : using our past to generate a future*. Oxford University Press.

Bartlett, F. C., & Bartlett, F. C. (1995). *Remembering: A study in experimental and social psychology*. Cambridge university press. http://pubman.mpdl.mpg.de/pubman/item/escidoc:2273030:5/component/escidoc:2309291/Bartlett_1932_Remembering.pdf

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*.

Benyamini, Y., McClain, C. S., Leventhal, E. A., & Leventhal, H. (2003). Living with the worry of cancer: Health perceptions and behaviors of elderly people with self, vicarious, or no history of cancer. *Psycho-Oncology*, *12*(2), 161–172. https://doi.org/10.1002/pon.637

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864.

Carbonell, J. G. (1983). Learning By Analogy: Formulating and Generalizing Plans From Past Experience. *Machine Learning*, *3597*, 137–161. https://doi.org/10.1016/b978-0-08-051054-5.50009-1

Carver, C. S., Scheier, M. F., & Weintraub, J. K. (1989). Assessing coping strategies: a theoretically based approach. *Journal of Personality and Social Psychology*, *56*(2), 267.

Cervone, D. (2000). Thinking about self-efficacy. *Behavior Modification*, *24*(1), 30–56.

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.

Chandran, S., & Menon, G. (2004). When a day means more than a year: Effects of temporal framing on judgments of health risk. *Journal of Consumer Research*, *31*(2), 375–389.

Chen, C. C., & Greene, P. G. (1998). Does entrepreneurial self-efficacy distinguish entrepreneurs from managers? *Journal of Business Venturing*, *13*(4), 295–316.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302.

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

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189–211.

Conner, M., & Norman, P. (1995). The role of social cognition models in predicting health behaviours: future directions. *Predicting Health Behaviour: Research and Practice with Social Cognition Models.*, 1–45.

Crossler, R., & Bélanger, F. (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.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226.

Daoud, J. I. (2017). Multicollinearity and regression analysis. *Journal of Physics: Conference Series*, *949*(1), 12009.

Darr, E. D., Argote, L., & Epple, D. (1995). The Acquisition, Transfer, and Depreciation of Knowledge in Service Organizations: Productivity in Franchises. *Management Science*, *41*(11), 1750–1762. https://doi.org/10.1287/mnsc.41.11.1750

Davis, K. (2003). Multiple analysis of variance (MANOVA) or multiple analysis of covariance (MANCOVA). *Unpublished Manuscript, Education Leadership and Research Department, Louisiana State University*.

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

Dhar, R., & Kim, E. Y. (2007). Seeing the forest or the trees: Implications of construal level theory for consumer choice. *Journal of Consumer Psychology*, *17*(2), 96–100.

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

Djafarova, E., & Rushworth, C. (2017). Exploring the credibility of online celebrities' Instagram profiles in influencing the purchase decisions of young female users. *Computers in Human Behavior*, *68*, 1–7. https://doi.org/10.1016/j.chb.2016.11.009

Dupuis, M, Crossler, R., & Endicott-Popovsky, B. (2012). The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information. *The Dewald Roode Information Security Workshop, Provo, Utah*.

Dupuis, Marc, Crossler, R., & Endicott-Popovsky, B. (2012). The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information. *The Dewald Roode Information Security Workshop, Provo, Utah*.

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.

Fazio, R. H., Chen, J.-M., McDonel, E. C., & Sherman, S. J. (1982). Attitude accessibility, attitude-behavior consistency, and the strength of the object-evaluation association. *Journal of Experimental Social Psychology*, *18*(4), 339–357.

Fazio, R. H., & Zanna, M. P. (1978). On the predictive validity of attitudes: The roles of direct experience and confidence. *Journal of Personality*, *46*(2), 228–243.

Fleischmann, M., Amirpur, M., Benlian, A., & Hess, T. (2014). Cognitive biases in information systems research: A scientometric analysis. *In Proceedings of the European Conference on Information Systems (ECIS) 2014*. http://aisel.aisnet.org/ecis2014/proceedings/track02/5

Floyd, D. L., Prentice ‐ Dunn, S., & Rogers, R. W. (2000). A meta ‐ analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fodor, J. A. (1975). *The language of thought* (Vol. 5). Harvard university press.

Fodor, J. A. (1985). Fodor's guide to mental representation: The intelligent auntie's vade-mecum. *Mind*, *94*(373), 76–100.

Fornell, C., & Larcker, D. F. (1981). *Structural equation models with unobservable variables and measurement error: Algebra and statistics*. Sage Publications Sage CA: Los Angeles, CA.

Foth, M., Schusterschitz, C., & Flatscher‐Thöni, M. (2012). Technology acceptance as an influencing factor of hospital employees' compliance with data‐protection standards in Germany. *Journal of Public Health*, *20*(3), 253–268.

Frank, M., & Kohn, V. (2023). Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. *Computers and Security*, *132*, 103386. https://doi.org/10.1016/j.cose.2023.103386

Freiman, J. A., Chalmers, T. C., Smith, H. A., & Kuebler, R. R. (2019). The importance of beta, the type II error, and sample size in the design and interpretation of the randomized controlled trial: survey of two sets of "negative" trials. In *Medical uses of statistics* (pp. 357–389). CRC Press.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 5.

Gino, F., Argote, L., Miron-Spektor, E., & Todorova, G. (2010). First, get your feet wet: The effects of learning from direct and indirect experience on team creativity. *Organizational Behavior and Human Decision Processes*, *111*(2), 102–115. https://doi.org/10.1016/j.obhdp.2009.11.002

Global Mobile Threat Report 2023. (2023). *ZIMPERIUM*.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users. *Information & Management*, *20*(1), 13–27. https://doi.org/10.1016/0378-7206(91)90024-v

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *Data Base for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. *In Proceedings of the International Conference on Information Systems, {ICIS} 2013*. https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/9

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis. In *Multivariate data analysis* (7th ed.). Prentice Hall.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16.

Hayes, A. F., Preacher, K. J., & Myers, T. A. (2011). Mediation and the estimation of indirect effects in political communication research. *Sourcebook for Political Communication Research: Methods, Measures, and Analytical Techniques*, *23*(1), 434–465.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84.

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.

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security*, *87*, 101594. https://doi.org/10.1016/j.cose.2019.101594

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit. *Articles*, 2.

Hopp, T., & Gangadharbatla, H. (2016). Novelty Effects in Augmented Reality Advertising Environments: The Influence of Exposure Time and Self-Efficacy. *Journal of Current Issues and Research in Advertising*, *37*(2), 113–130. https://doi.org/10.1080/10641734.2016.1171179

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.

Jaeger, L., Ament, C., & Eckhardt, A. (2017). The Closer You Get the More Aware You Become–A Case Study about Psychological Distance to Information Security Incidents. *In Proceedings of the International Conference on Information Systems - Transforming Society with Digital Innovation, {ICIS} 2017. Association for Information Systems*.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 196–213.

Johnson, D. H. (1999). The insignificance of statistical significance testing. *The Journal of Wildlife Management*, 763–772.

Johnson, M. K., Hashtroudi, S., & Lindsay, D. S. (1993). Source monitoring. *Psychological Bulletin*, *114*(1), 3.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 549–566.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences*, *50*(2), 245–284.

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

Jones, L. W., Sinclair, R. C., & Courneya, K. S. (2003). The effects of source credibility and message framing on exercise intentions, behaviors, and attitudes: an integration of the elaboration likelihood model and prospect theory 1. *Journal of Applied Social Psychology*, *33*(1), 179–196.

Kahneman, D., & Lovallo, D. (1993). Timid choices and bold forecasts: A cognitive perspective on risk taking. *Management Science*, *39*(1), 17–31.

Kantowitz, B. H., Roediger III, H. L., & Elmes, D. G. (2014). *Experimental psychology*. Nelson Education.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 3.

Kellens, W., Zaalberg, R., Neutens, T., Vanneuville, W., & De Maeyer, P. (2011). An Analysis of the Public Perception of Flood Risk on the Belgian Coast. *Risk Analysis*, *31*(7), 1055–1068. https://doi.org/10.1111/j.1539-6924.2010.01571.x

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal*, *22*(4), 171–179. https://doi.org/10.1080/19393555.2013.828803

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

Koehler, D. J. (1991). Explanation, imagination, and confidence in judgment. *Psychological Bulletin*, *110*(3), 499.

Krueger, N., & Dickson, P. R. (1994). How Believing in Ourselves Increases Risk Taking: Perceived Self ‐ Efficacy and Opportunity Recognition. *Decision Sciences*, *25*(3), 385–400. https://doi.org/10.1111/j.1540-5915.1994.tb01849.x

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1–31.

Lantz, B. (2013). The large sample size fallacy. *Scandinavian Journal of Caring Sciences*, *27*(2), 487–492.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer publishing company.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454.

Leventhal, H. (1970). Findings and theory in the study of fear communications. In *Advances in experimental social psychology* (Vol. 5, pp. 119–186). Elsevier.

Li, Y., Xin, T., & Siponen, M. (2022). Citizens' Cybersecurity Behavior: Some Major Challenges. *IEEE Security and Privacy*, *20*(1), 54–61. https://doi.org/10.1109/MSEC.2021.3117371

Li, Y., Zhang, N., & Siponen, M. (2019). Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation. *Behaviour & Information Technology*, *38*(5), 435–453.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, 71–90.

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

Liberman, N., & Förster, J. (2008). Expectancy, value and psychological distance: A new look at goal gradients. *Social Cognition*, *26*(5), 515.

Liberman, N., Trope, Y., & Stephan, E. (2007). Psychological distance. *Social Psychology: Handbook of Basic Principles*, *2*, 353–383.

Liberman, N., Trope, Y., & Wakslak, C. (2007). Construal level theory and consumer behavior. *Journal of Consumer Psychology*, *17*(2), 113–117.

Lin, Y.-Y., Hsu, H.-M., & Hsu, S.-C. (2019). A study of the Effects of Information Security Advocacy. *PACIS 2019 Proceedings*, 58.

Lin, Y. C., Liang, J. C., Yang, C. J., & Tsai, C. C. (2013). Exploring middle-aged and older adults' sources of Internet self-efficacy: A case study. *Computers in Human Behavior*, *29*(6), 2733–2743. https://doi.org/10.1016/j.chb.2013.07.017

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

Luuk, B., (Maria) Susanne, V. H. de G., Ellen, M. ter H., Ynze, V. H., Remco, S., & Eric Rutger, L. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers and Security*, *127*, 103099. https://doi.org/10.1016/j.cose.2023.103099

Mady, A., & Gupta, S. (2017). Behavioral Approach to Information Security Policy Compliance. *In Proceedings of the 23th Americas Conference on Information Systems*. https://api.semanticscholar.org/CorpusID:150379443

Maloney, E. K., Lapinski, M. K., & Witte, K. (2011). Fear appeals and persuasion: A review and update of the extended parallel process model. *Social and Personality Psychology Compass*, *5*(4), 206–219.

Mccarthy, G. (2018). *Introduction to Metaphysics*. Scientific e-Resources.

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological Methods*, *17*(3), 437.

Messier, W. F., Hibbs, R. M., Messier Jr, W. F., & Tubbs, R. M. (1994). Recency Effects in Belief Revision: The Impact of Audit Experience and the Review Process. *Auditing*, *13*(1), 57–72. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9703131783&site=ehost-live

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.

Milne, S., Sheeran, P., & Orbell, S. (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., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1).

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, *135*(May), 113323. https://doi.org/10.1016/j.dss.2020.113323

Murdock, M. R., & Rajagopal, P. (2017). The sting of social: how emphasizing social consequences in warning messages influences perceptions of risk. *Journal of Marketing*, *81*(2), 83–98.

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. *In 47th Hawaii International Conference on System Sciences, {HICSS} 2014*, 3188–3197. https://doi.org/10.1109/HICSS.2014.396

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.

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. *Journal of Management Information Systems*, *38*(3), 732–764. https://doi.org/10.1080/07421222.2021.1962601

Norman, K. A., & Reilly, R. C. O. (2003). Modeling hippocampal and neocortical contributions to recognition memory: a complementary-learning-systems approach. *Psychological Review*, *110*(4), 611.

Norris, F. H., & Murrell, S. A. (1988). Prior experience as a moderator of disaster impact on anxiety symptoms in older adults. *American Journal of Community Psychology*, *16*(5), 665–683.

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

Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal-level Theory in Designing Fear Appeals in IS Security Research. *Communications of the Association for Information Systems*, *45*(1), 22.

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological Bulletin*, *124*(1), 54.

Perugini, M., & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal-directed behaviours: Broadening and deepening the theory of planned behaviour. *British Journal of Social Psychology*, *40*(1), 79–98. https://doi.org/10.1348/014466601164704

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, *21*. https://doi.org/10.3127/ajis.v21i0.1321

Pitt, D. (2000). *Mental representation*. The Stanford Encyclopedia of Philosophy (Fall 2022 Edition). https://plato.stanford.edu/archives/fall2022/entries/mental-representation/

Pornpitakpan, C. (2004). The persuasiveness of source credibility: A critical review of five decades' evidence. *Journal of Applied Social Psychology*, *34*(2), 243–281. https://doi.org/https://doi.org/10.1111/j.1559-1816.2004.tb02547.x

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, *40*(3), 879–891.

Preacher, K. J., Rucker, D. D., & Hayes, A. F. (2007). Addressing moderated mediation hypotheses: Theory, methods, and prescriptions. *Multivariate Behavioral Research*, *42*(1), 185–227.

Read, D., & Grushka-Cockayne, Y. (2011). The similarity heuristic. *Journal of Behavioral Decision Making*, *24*(1), 23–46. https://doi.org/10.1002/bdm.679

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826.

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.

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). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook* (pp. 153–177).

Rogers, R. W., Prentice-Dunn, S., & Gochman, D. S. (1997). *Handbook of health behavior research 1: personal and social determinants*. New York, NY, US: Plenum Press.

Ruiter, R. A. C., Abraham, C., & Kok, G. (2001). Scary warnings and rational precautions: A review of the psychology of fear appeals. *Psychology and Health*, *16*(6), 613–630.

Ruiter, R. A. C., Kessels, L. T. E., Peters, G. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, *49*(2), 63–70.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78.

Schacter, D. L., & Addis, D. R. (2007). The cognitive neuroscience of constructive memory: Remembering the past and imagining the future. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *362*(1481), 773–786. https://doi.org/10.1098/rstb.2007.2087

Schuetz, S., Lowry, P. B., & Thatcher, J. (2016). Defending against spear-phishing: Motivating users through fear appeal manipulations. *In 20th Pacific Asia Conference on Information Systems, {PACIS} 2016*.

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723–757.

Schuetz, S. W., Lowry, P. B., Pienta, D., & Thatcher, J. (2020). Improving the design of information security messages by leveraging the effects of temporal distance and argument nature. *Journal of the Association for Information Systems (JAIS)*, *22*(5), 1376–1428.

Sherman, S. J., Cialdini, R. B., Schwartzman, D. F., & Reynolds, K. D. (1985). Imagining can heighten or lower the perceived likelihood of contracting a disease: The mediating effect of ease of imagery. *Personality and Social Psychology Bulletin*, *11*(1), 118–127.

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2023). Protection Motivation Theory in Information Security Behavior Research: Reconsidering the Fundamentals. *Communications of the Association for Information Systems*, *53*(1), 47. https://doi.org/10.17705/1CAIS.044XX

Siponen, M. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society*, *31*(2), 24–29. https://doi.org/10.1145/503345.503348

Siponen, M., Klaavuniemi, T., & Xiao, Q. (2023). Splitting versus lumping: narrowing a theory's scope may increase its value. *European Journal of Information Systems*, *00*(00), 1–10. https://doi.org/10.1080/0960085X.2023.2208380

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. *In New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22 Nd International Information Security Conference (SEC 2007),14–16 May 2007, Sandton, South Africa 22 (Pp. 133-144). Springer US*, 133–144. https://doi.org/https://doi.org/10.1007/978-0-387-72367-9_12

Siponen, M. T. (2000). Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behavior. *PACIS*, 31.

Sterelny, K. (1990). *The representational theory of mind: An introduction*. Basil Blackwell.

Sternberg, R. J., & Sternberg, K. (2011). *Cognitive psychology*. Cengage Learning.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(1), 24.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244.

Taylor, S. E., Kemeny, M. E., Aspinwall, L. G., Schneider, S. G., Rodriguez, R., & Herbert, M. (1992). Optimism, coping, psychological distress, and high-risk sexual behavior among men at risk for acquired immunodeficiency syndrome (AIDS). *Journal of Personality and Social Psychology*, *63*(3), 460.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly: Management Information Systems*, *19*(4), 561–568. https://doi.org/10.2307/249633

Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, *4*(2), 142–168.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391.

Tourangeau, R., Rips, L. J., & Rasinski, K. (2000). *The psychology of survey response*. Cambridge University Press.

Trope, Y, & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychol Rev*, *117*(2), 440–463. https://doi.org/10.1037/a0018963

Trope, Yaacov, & Liberman, N. (2003). Temporal construal. *Psychological Review*, *110*(3), 403.

Trope, Yaacov, & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, *117*(2), 440. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3152826/pdf/nihms314649.pdf

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.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, *52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52*(4), 506–517.

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud and Security*, *2006*(6), 17–19. https://doi.org/10.1016/S1361-3723(06)70370-0

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), 2.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. *In 2013 46th Hawaii International Conference on System Sciences*, 2988–2997.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Von Eckardt, B. (2012). The representational theory of mind. In *The Cambridge handbook of cognitive science* (Vol. 1).

Wall, J. D., & Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*, *56*(8), 103157.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems*, *17*(3), 194.

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, *39*(5), 806.

Weinstein, N. D. (1989). Effects of personal experience on self-protective behavior. *Psychological Bulletin*, *105*(1), 31.

Williams, M. (1984). Language learning and the representational theory of mind. *Synthese*, *58*(2), 129–151. https://www.jstor.org/stable/20115962

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.

Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human Computer Studies*, *128*, 61–71. https://doi.org/10.1016/j.ijhcs.2019.02.003

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Wurtele, S. K., & Maddux, J. E. (1987). Relative contributions of protection motivation theory components in predicting exercise intentions and behavior. *Health Psychology*, *6*(5), 453.

Xie, Y. (2022). A Multi-Theoretical Perspective on Conceptualization and Contextualization of IS Security Behavior. *JYU Dissertations*.

Xin, T., Siponen, M., & Chen, S. (2022). Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats. *Behaviour and Information Technology*, *41*(13), 2835–2859. https://doi.org/10.1080/0144929X.2021.1954242

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401–419.

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.

Zhang, X., Han, X., Dang, Y., Meng, F., Guo, X., & Lin, J. (2017). User acceptance of mobile health services from users' perspectives: The role of self-efficacy and response-efficacy in technology acceptance. *Informatics for Health and Social Care*, *42*(2), 194–206. https://doi.org/10.1080/17538157.2016.1200053