JYU DISSERTATIONS 534

Yitian Xie

A Multi-Theoretical Perspective on Conceptualization and Contextualization of IS Security Behavior

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 534

Yitian Xie

A Multi-Theoretical Perspective on Conceptualization and Contextualization of IS Security Behavior

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Ruusupuiston salissa D104 (Helena)
kesäkuun 7. päivänä 2022 kello 15.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Ruusupuisto, hall D104 (Helena), on June 7, 2022 at 15 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2022

Editors
Mikko Siponen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-951-39-9317-7 (PDF)
URN:ISBN:978-951-39-9317-7
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-9317-7

ABSTRACT

Xie, Yitian
A multi-theoretical perspective on conceptualization and contextualization of IS security behavior
Jyväskylä: University of Jyväskylä, 2022, 49 p.
(JYU Dissertations
ISSN 2489-9003; 534)
ISBN 978-951-39-9317-7 (PDF)

The Internet has connected almost everything in our daily life, making information systems security (ISec) an important issue not only to organizations but also to personal users. Despite the increasing number of users of Internet-connected IT, there is insufficient research into how users make their ISec-related decisions (i.e., the cognitive appraisals), their decision-making process under the influence of emotion (i.e., the emotional motivation), user characteristics (e.g., user involvement, years of use), or whether they have enough ISec knowledge to make the right decision to secure their information and computing environment (i.e., the knowledge level).

This dissertation contributes to bridging these research gaps by focusing on three studies that explore the security-related decision-making process among personal users. By using novel theoretical perspectives and revisiting some of the "old" theoretical assumptions, we offer insights of value to both academics and practitioners. Three studies are tested and reported that provide insights into the cognitive appraisals, emotional motivation, user characteristics, and ISec knowledge of personal users' decision-making process regarding security-related behavior.

By considering additional theories and constructs and revisiting the theoretical and methodology perspectives, this dissertation provides several contributions to behavioral ISec studies. The results of the empirical study provide new insights into the cognitive mediation process, the decision-making process under the influence of defensive avoidance, and personal users' self-regulated ability to protect their personal computing devices.

Keywords: cognitive mediation, defensive avoidance, information security knowledge, threat appeals, boundary condition, conceptualization, instrument development

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Xie, Yitian
Moniteoreettinen näkökulma tietoturvakäyttäytymisen käsitteellistämiseen ja kontekstualisointiin
Jyväskylä: University of Jyväskylä, 2022, 49 p.
(JYU Dissertations
ISSN 2489-9003; 534)
ISBN 978-951-39-9317-7 (PDF)

Internet on yhdistänyt lähes kaiken jokapäiväisessä elämässämme, mikä tekee tietojärjestelmien turvallisuudesta tärkeän kysymyksen paitsi organisaatioille myös henkilökohtaisille käyttäjille. Huolimatta Internetiin yhdistetyn IT:n käyttäjien lisääntyvästä määrästä, ei ole riittävästi tutkittu sitä, kuinka käyttäjät tekevät tietoturvaan liittyviä päätöksiä (eli kognitiivinen arviointi), miten tunteet vaikuttavat heidän päätöksentekoprosessiinsa (eli tunnevaikutus), millaisia ovat käyttäjän ominaisuudet (esim. käyttäjän osallistuminen, käyttövuodet) tai onko heillä tarpeeksi tietoturvatietoa tehdäkseen oikean päätöksen tieto- ja laskentaympäristönsä turvaamiseksi (eli tietotaso).

Tämä väitöskirja auttaa osaltaan kuromaan umpeen näitä tutkimusaukkoja keskittymällä kolmeen tutkimukseen, joissa tutkitaan turvallisuuteen liittyvää päätöksentekoprosessia henkilökohtaisten käyttäjien keskuudessa. Käyttämällä uusia teoreettisia näkökulmia ja tarkastelemalla uudelleen joitakin ”vanhoja” teoreettisia olettamuksia tarjoamme arvokkaita oivalluksia sekä tutkijoille että käytännön toimijoille. Testatut ja raportoidut kolme tutkimusta tarjoavat käsityksen kognitiivisista arvioista, emotionaalisista vaikutuksista, käyttäjien ominaisuuksista ja tietoturvatietoisuudesta henkilökohtaisten käyttäjien turvallisuuteen liittyvän käyttäytymisen päätöksentekoprosessissa.

Käsittelemällä muita teorioita ja konstruktioita sekä tarkastelemalla uudelleen teoreettisia ja metodologisia näkökulmia tämä väitöskirja tarjoaa useita panoksia tietoturvakäyttäytymistutkimuksiin. Empiirisen tutkimuksen tulokset antavat uusia näkemyksiä kognitiiviseen mediaatioprosessiin, päätöksentekoprosessiin puolustavan välttämisen vaikutuksesta sekä henkilökohtaisten käyttäjien itsesäätelevään kykyyn suojata henkilökohtaisia tietokonelaitteitaan.

Avainsanat: kognitiivinen mediaatio, puolustava välttäminen, tietoturvatieto, uhkien vetoomukset, rajaehto, käsitteellisyys, instrumenttien kehittäminen

Author
Yitian Xie
Faculty of Information Technology
University of Jyväskylä
Finland
ORCID: 0000-0002-1497-7547

Supervisors
Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers
Huigang Liang
University of Memphis
USA

Xin Luo
University of New Mexico
USA

Opponent
Carol Hsu
University of Sydney
Australia

ACKNOWLEDGEMENTS

First, I would like to acknowledge the guidance that Prof. Mikko Siponen has provided for the body of this work. With his insights, especially into philosophical perspective regarding information systems security studies. With his patience and meticulous guidance, I have been able to accomplish my doctoral studies in Finland and explore several interesting research questions in the behavioral information security field.

I want to express my sincere thankfulness for the kindly help and valuable advice offered by two co-authors of the work, Prof. Gregory Moody, and Prof. Xiaosong Zheng.

I would like to thank all the reviewers and colleagues who provided constructive feedback for these studies. Thank Marja-Leena Rantalainen and Nina Pekkala for your help in formatting this dissertation.

I also appreciate all the help and support for my mental wellbeing from Prof. Mikko Siponen, Dr. Tuula Klaavuniemi, Ella-Leena Anttila, and Tarja Orenius during the pandemic.

Last but not least, I would like to thank the external reviewers of this thesis, namely Prof. Huigang Liang and Prof. Xin (Robert) Luo, for their insightful comments concerning my doctoral thesis.

Jyväskylä 31. 12.2021
Yitian Xie

FIGURES

TABLES

ABBREVIATIONS

BC	Boundary Condition
CBSEM	Covariance-based Structural Equation Modeling
CM	Cognitive Mediation
CMs	Multiple Cognitive Mediation
DV	Dependent Variable
EPPM	Extended Parallel Process Model
INFOSEC	Information Security
IS	Information Systems
ISEC	Information Systems Security
ISK	Information Security Knowledge
IT	Information Technology
IV	Independent Variable
ME	Mediation Variable
MCM	Multiple Mediation Mechanism
P (P_M)	The Ratio of the Indirect Effect to the Total Effect
PMT	Protection Motivation Theory
PRM	Parallel Response Model
R (R_M)	The Ratio of the Indirect Effect to the Direct Effect
SMFAS	Stage Model of Fear-arousing Communication Processing
TTAT	Technology Threat Avoidance Theory
UI	User Involvement
VEL	Perceived Vulnerability

CONTENTS

LIST OF INCLUDED ARTICLES

I Xie, Y., Siponen, M., Moody, G., & Zheng, X. The cognitive mediation process in threat-based theories in IS security. Major revision in *Computers & Security*.

II Xie, Y., Siponen, M., Moody, G., & Zheng, X. (2022). Discovering the interplay between defensive avoidance and continued use intention of anti-malware software among experienced home users: A moderated mediation model. *Information & Management*, *59*(2), 103586.

III Xie, Y., & Siponen, M. Declarative and procedural information security knowledge of the general public: Conceptualization and instrument development. Unpublished Manuscript.

1 INTRODUCTION

The increased connectivity of the Internet makes information systems security (ISec) an essential concern not only for corporations and organizations (Aurigemma & Mattson, 2017; Boss et al., 2015; Chen et al. 2021; Moody et al., 2018; Johnston et al., 2015; Vance et al. 2012) but also for personal users (Anderson & Agarwal., 2010; Chen & Zahedi, 2016; Liang et al. 2019; Xin et al., 2021; Li et al., 2019). Without the facilitation of the IT personnel support, security environment set-up, and information security policy regulation, which is available in organizational contexts, ISec outside such contexts (e.g., in households) mostly relies on personal users' information security awareness, protection motivation, and adequate competence to execute security-related protections (e.g., Li & Siponen, 2011; Li et al., 2022). Extant research examining ISec has largely applied theories from other disciplines (Siponen & Baskerville 2018; Karjalainen et al. 2019, 2020), in particular from criminology (e.g., Luo et al. 2020; Straub 1990; Vance et al. 2020), moral psychology (Li et al. 2021; Myyry et al., 2009), health psychology (e.g., Aurigemma & Mattson, 2017; Haag et al., 2021; Liang et al., 2019), and moral philosophy (Siponen, 2001).

This doctoral thesis particularly focuses on, and contributes to, the application of health psychology theories in ISec. Despite progress made by existing research investigating how personal users make (or intend to make) protection behavior-related decisions, a better understanding of how personal users make such decisions in their daily life is still required. This dissertation attempts to explore several main research questions, discussed in the next section, by looking at a variety of security-related cognitions, emotions, and competences of personal users from different theoretical perspectives.

Boundary condition (BC) depicts a constraint condition that depicts the ''who, where, when'' aspects of a theory (Whetten, 1989). Besides the static perspective above, Busse et al. noted a dynamic perspective of BC as follows:

> The dynamic perspective on BC directs attention to the process of exploring BC, which it considers as a research effort directed at making BC more certain. Moreover, it views the exploration of BC as intimately intertwined with the theory development process.

> It suggests that the exploration of BC can be regarded as an instrument (i.e., means) for further development of the respective theory. (Busse et al., 2017, p. 581)

Busse et al. (2017) contend the amendment of mediators, the amendment of moderators, and refinement of constructs as three "methodologically equivalent" tool of the exploration of boundary condition (BC).

1.1 Approaches for Boundary Condition Exploration

An essential objective of this dissertation is to explore the boundary conditions of theories that are widely used in ISec studies in three different empirical studies. To this end, three studies were designed to examine security-related behavior in different contexts, each from its own theoretical perspective. Each of the three studies is briefly summarized here.

1.1.1 Theoretical and Methodological Reconsideration of the Cognitive Mediation Assumption in Threat-based Theories in IS Security

Threat theories, often called as fear appeals, are known and widely studies in IS (Aurigemma & Mattson., 2019; Boss et al., 2015; Burns et al., 2017; Chen et al. 2021; Chen & Zahedi, 2016; Crossler et al., 2014; Johnston et al. 2015; Moodey et al. 2018; Posey, Roberts & Lowry., 2015; Vance et al., 2012). In Article I, we point out that the *cognitive mediation (CM)* process has been a fundamental theoretical assumption for threat theories for more than 50 years (Hovland et al., 1953; Janis & Feshbach, 1967; McGuire, 1968). For example, the pioneering threat theorists, such as Howard Leventhal (1970), Ronald W. Rogers (1975, 1985), Kim, Malhotra, and Narasimhan (2005), and Witte (1992, 1994), all deemed the CM process to be a key component of their theories. Recently, interest in ISec has grown to scrutinize and debate the fundamental assumptions of these theories, especially in the case of PMT (Aurigemma et al., 2019; Boss et al., 2015; Johnston et al., 2015). However, the CM assumption, albeit being a fundamental theoretical assumption in many threat theories discussed and applied in ISec, has been overlooked in IS security research either fully or in detail. The qualifying locution "in detail" means that while some ISec scholars have referred to the CM process (e.g., Martens et al., 2019; Tu et al., 2015; Vance, Siponen, & Pahnila, 2012; Verkijika, 2018), they have not tested it as such (i.e., as CM process). More specifically, we report three underutilized cases where the insights on CM assumptions can shed new light on ISec research.

Testing CM assumptions could offer important information on theory testing and even for theory building, which is in fact recognized by many authors outside of Information Systems (Cook & Groom, 2004; Rucker, Preacher, Tormala, and Petty, 2011; Vanderweele & Vansteelandt, 2009; Zhao, Lynch, and Chen, 2010). For instance, as for theory testing, the result of a CM test can determine the form of the theoretical model by offering significant indirect and direct effect results. Also, testing CM, as commonly noted in statistical mediation literature, can offer theory-building suggestions (Rucker et al., 2011; Zhao, Lynch, and Chen, 2010). More broadly, it is commonly that in sciences generally, hypothesis or theory building can come from similar or findings (Siponen & Klaavuniemi 2020).

In addition, multiple mediation analysis facilitates theories/constructs comparison because it includes two (or more) mediators in one model. One can then compare the strengths of two (or more) indirect effects to decide which theory (or construct) should be given more credence. For researchers who are interested in comparing rivaling theories or constructs, the multiple mediation assumption and test can offer a better practice for such comparisons than simple mediation or SEM solely.

Accordingly, in Article I, we first explain how CM figures in as a key theoretical assumption of the threat theories. Importantly, while CM is ultimately a fundamental theory assumption rather than merely a statistical issue, there is a necessity to distinguish CM as a theory assumption and CM as a statistical method (Preacher & Hayes, 2008; Pirlott & Mackinnon, 2016; Rucker, Preacher, Tormala, & Petty, 2011; Vanderweele & Vansteelandt, 2009; Zhao, Lynch, & Chen, 2010). While CM does not need to be examined in every paper, understanding CM is important to many of those applying threat theories, such as PMT (2) or EPPM. Moreover, to illustrate the use of CM as a theoretical assumption and CM as a statistical method, we propose a two-mediator model and empirically compare the CM process initiated from three different prior coping responses initiate by internal cues that the experienced users may encounter during the use of anti-malware in their home computer(s).

1.1.2 Moderation Role of User Involvement and Perceived Vulnerability on the CMs among Defensively Motivated Home Users

Most of *classic fear appeal theories* also herein discussed as threat theories, assume an objective and information-based message processing mode for the cognitive mediation process (Rogers & Mewborn, 1976; Rippetoe & Rogers, 1987). Take protection motivation theory (Rogers 1975, 1983) as an example, it assumes a linear relationship between the cognitive appraisals' factors and the cognitive outcome. For example, an increased perception of the severity of a threat may lead to increased protection motivation and protection behavior (Anderson & Agarwal, 2010). Another example is that an increased perception of response cost may lead to decreased protection motivation and protection behavior (Siponen et al., 2010). In short, all cognitive mediation processes based on the classic fear appeal proposed an objective and information-based message processing mode.

However, we, as human beings, are not always been so objective and rational. Instead, we usually processing information in biased way under the influence of our preoccupied beliefs or even prejudice (Das, de Wit, & Stroebe., 2003; de Hoog et al., 2008).

Based on this, a stage model of fear-arousing communication (Das et al., 2003; de Hoog et al., 2005, 2007, 2008; de Wit et al., 2007), therefore, proposes a biased information processing mode initiated by defensively motivated individuals. A stage model of fear-arousing communication is briefly termed as the stage model. It assumes that the way in which people process a fear-arousing message is determined by their processing motivation. According to stage model, individuals exposed to fear-arousing communication will engage in two types of appraisals in sequence: an appraisal of the threat and an appraisal of the coping strategies available for reducing the threat (Das et al., 2003; de Hoog et al., 2005, 2007, 2008). Only if a threat is perceived to be relevant and potentially harmful will an appraisal of efficacy occur. In addition, the stage model, besides the cognitive mediation research propositions, also depicts a "when" condition or a boundary condition of fear-arousing communication under the influence of defensive avoidance motivation (Das et al., 2003; de Hoog et al., 2005, 2007, 2008).

Our results suggest that information that raises high user involvement or makes an individual feel vulnerable to a self-relevant nontrivial threat (e.g., malware's compromise of their home computer) is likely to induce a negative processing bias in the primary appraisal process (i.e., the severity of the malware threat) and a positive processing bias in the secondary appraisal process (i.e., the efficacy of the protection action).

1.1.3 Decomposition of the Generic Conceptual Definition and Measurement of Information Security Knowledge

As noted by Busse et al.,

> *Boundary condition*-related refining of constructs will often entail splitting one rather general into multiple more specific constructs. Because of the increase in specificity of the constructs' meanings, each of the resulting constructs can subsequently be measured more precisely, thereby fostering the accuracy of the respective theory and its generalizability across contexts. (Busse et al., 2017, pp. 587–588)

Information security knowledge (ISK) is an essential premise for citizens' information security (infosec) awareness and infosec behavior. Most previous studies assess ISK with generic measures. In measuring ISK, they omit numerous characteristics. These include omitting the fact that infosec includes security enhancement and risk avoidance approaches. In addition, existing measures do not differentiate adequately between declarative knowledge and procedural knowledge. To improve the contextual and practical relevance of the field survey, echoing the call from Siponen and Vance (2014), this study decomposes ISK into four sub-constructs that aimed at capturing the multidimensional characteristics of ISK and guide future instrument development and validation.

Drawing from cybernetics theory, previous studies identified two self-regulating behavior tendencies, goal pursuit and anti-goal avoidance (Carver, 2006; Carver & Scheier, 1982, 1998, 2012). Contextualize these two behavioral tendencies into infosec context, goal pursuit refers to infosec enhancement (e.g., using anti-malware software). In turn, anti-goal avoidance refers to risk avoidance (e.g., avoid clicking malicious links; Liang & Xue, 2009). However, a lack of related ISK may hinder people from executing infosec behavior through these two approaches. In this study we conceptualized declarative and procedural ISK under infosec enhancement and risk avoidance scenarios. In addition, we developed an instrument to measure declarative and procedural ISK.

The developed instrument tested with 1045 participants captures ten infosec topics in the personal information security context. New contributions are the following: 1) decompose and conceptualize ISK as declarative security or risk knowledge and procedural security or risk knowledge, and 2) empirically test the hierarchical relation of the four sub-constructs of ISK and develop an instrument for measuring them. The study offers practical and theoretical implications for infosec practice and research.

1.2 Publication Status

This dissertation consists of three articles, one of which has been published and two under review in a journal. The status of the articles is shown in Table 1.

TABLE 1 Publishing status of the included articles

Article	Co-Author(s)	Status
I	Mikko Siponen, Gregory Moody, Xiaosong Zheng	*Computers & Security*, major revision
II	Mikko Siponen, Gregory Moody, Xiaosong Zheng	*Information & Management*, published
III	Mikko Siponen	Unpublished manuscript.

2 OVERVIEW OF INCLUDED ARTICLES

2.1 Article I: The Cognitive Mediation Process in Threat-based Theories in IS Security

Xie, Y., Siponen, M., Moody, G., & Zheng, X. The cognitive mediation process in threat-based theories in IS security. Major revision in *Computers & Security*.

2.1.1 Method of Article I

We performed a percentile-based bootstrap confidence interval (CI) and a bias-corrected (BC) bootstrapping CI with 5,000 iterations to examine whether the mediation effects exist (Hayes, 2009; Preacher & Hayes, 2008; Zhao, Lynch, & Chen, 2010). The standard error (SE), critical ratios, and percentile-based bootstrap CI for these effects are reported in Table 2.

In addition, we further examined the decomposition of mediation effect, which provided more detailed information regarding the CM models (Lau & Cheung, 2012). As shown in Table 3, we can conclude that (1) Model 3 has achieved the largest indirect effect among the three models, and (2) that the effect size of the perceived threat is larger than the perceived efficacy in all three models; however, these distinctions did not achieve statistical significance.

TABLE 2 Decomposition effect size of multiple CMs

Effect size	Model 1	Model 2	Model 3
IV-Me$_1$ (Path a_1)	0.314***	0.359***	-0.410***
IV-Me$_2$ (Path a_2)	0.425***	0.414***	-0.382***
Me$_1$-DV (Path b_1)	0.269***	0.204***	0.231***
Me$_2$-DV (Path b_2)	0.170**	0.115**	0.222***
Direct effect (Path c')	0.342***	0.542***	-0.285***
Indirect effect (ab)	0.221	0.127	-0.230
Total effect (c)	0.702	0.696	-0.594
Specific indirect effect (PM$_1$)	0.119	0.077	-0.121
Specific indirect effect (PM$_2$)	0.102	0.050	-0.109
Ratio of the specific indirect effect (RM$_1$)	0.539	0.605	0.527
Ratio of the specific indirect effect (RM$_2$)	0.461	0.395	0.473
Contrast between two indirect paths (PM$_1$/PM$_2$)	ns	ns	ns

* p-value < 0.05; ** p-value < 0.01; *** p-value < 0.001; ns = not significant

The index of mediation effect size is represented following the suggestion of MacKinnon (2008) and Wen and Fan (2015). The report of the decomposition effect includes total effect (c), direct effect (c′), indirect effect (ab), P (P_M) (i.e., the ratio of the indirect effect to the total effect), R (R_M) (i.e., the ratio of the indirect effect to the direct effect), and the difference of specific indirect effect. The formula of the total effect (c), the ratio of the indirect effect to the total effect (P), and the difference of specific indirect effect (R) are

$$c = ab + c' , \quad P = \frac{ab}{c} , \quad R = \frac{ab}{c'} .$$

TABLE 3 Decomposition of multiple CMs

Point estimate	Product of coefficient		Bootstrap 5,000 times 95% CI			
			Bias-corrected		Percentile-based	
	SE	*Z*	Lower	Upper	Lower	Upper
Model 1: Automatic habitual behavior						
Specific indirect effect-perceived threat (P_M1)						
0.119	0.035	3.400	0.063	0.204	0.055	0.194
Specific indirect effect-perceived efficacy (P_M2)						
0.102	0.035	2.914	0.040	0.180	0.030	0.170
Indirect effect (ab)						
0.221	0.043	5.140	0.144	0.321	0.132	0.311
Direct effect (c′)						
0.482	0.083	5.807	0.324	0.648	0.335	0.661
Total effect (c)						
0.702	0.085	8.259	0.548	0.882	0.548	0.883
Specific effect difference						
-0.017	0.056	− 0.304	− 0.132	0.087	- 0.132	0.087
Perceived threat/Indirect effect (R_M1)						
0.539	0.133	4.053	0.293	0.827	0.295	0.829
Perceived efficacy/Indirect effect (R_M2)						
0.461	0.133	3.466	0.173	0.707	0.171	0.705

Point estimate	Product of coefficient		Bootstrap 5,000 times 95% CI			
			Bias-corrected		Percentile-based	
	SE	Z	Lower	Upper	Lower	Upper
Model 2: Past reasoned-based behavior						
Specific indirect effect-perceived threat (P_M1)						
0.077	0.024	3.208	0.037	0.130	0.034	0.126
Specific indirect effect-perceived efficacy (P_M2)						
0.050	0.022	2.273	0.010	0.099	0.007	0.094
Indirect effect (ab)						
0.127	0.026	4.885	0.084	0.190	0.080	0.179
Direct effect (c′)						
0.569	0.055	10.345	0.461	0.672	0.462	0.677
Total effect (c)						
0.696	0.050	13.920	0.598	0.792	0.599	0.793
Specific effect difference						
-0.027	0.038	− 0.711	− 0.106	0.043	- 0.105	0.044
Perceived threat/Indirect effect (R_M1)						
0.605	0.155	3.903	0.322	0.933	0.320	0.932
Perceived efficacy/Indirect effect (R_M2)						
0.395	0.155	2.548	0.067	0.678	0.068	0.680

SE: standard error; CI: confidence interval; $Z = \hat{a}\hat{b}/s_{ab}$, $\hat{a}$ and $\hat{b}$ are estimation of a and b, s_{ab} is the standard error of $\hat{a}\hat{b}$

(Table 3 continues)

Point estimate	Product of coefficient		Bootstrap 5,000 times 95% CI			
			Bias-corrected		Percentile-based	
	SE	*Z*	Lower	Upper	Lower	Upper
			Model 3: Defensive avoidance			
			Specific indirect effect-perceived threat (P_M1)			
− 0.121	0.037	− 3.270	− 0.202	− 0.059	− 0.200	− 0.054
			Specific indirect effect-perceived efficacy (P_M2)			
− 0.109	0.031	− 3.516	− 0.182	− 0.058	− 0.173	− 0.053
			Indirect effect (ab)			
− 0.230	0.042	− 5.476	− 0.328	− 0.160	− 0.319	− 0.151
			Direct effect (c′)			
− 0.364	0.075	− 4.853	− 0.516	− 0.220	− 0.524	− 0.226
			Total effect (c)			
− 0.594	0.073	− 8.137	− 0.737	− 0.459	− 0.737	− 0.459
			Difference of specific indirect effect			
0.012	0.054	0.222	− 0.098	0.117	− 0.093	0.122
			Perceived threat/Indirect effect (R_M1)			
0.527	0.117	4.504	0.269	0.742	0.287	0.765
			Perceived efficacy/Indirect effect (R_M2)			
0.473	0.117	4.043	0.258	0.731	0.235	0.713

SE: standard error; CI: confidence interval; $Z = \hat{a}\hat{b}/s_{ab}$, $\hat{a}$ and $\hat{b}$ are estimation of a and b, s_{ab} is the standard error of $\hat{a}\hat{b}$

2.1.2 Results of Article I

The results confirmed the existence of a positive and significant mediation effect for perceived threat in habit (mediation effect = 0.119, BC 95%; CI = [0.063, 0.204]) and perceived efficacy in habit (mediation effect = 0.102, BC 95%; CI = [0.040, 0.180]). The results confirmed the existence of a positive and significant mediation effect for perceived threat in past reasoned-based behavior (mediation effect = 0.077, BC 95%; CI = [0.037, 0.130]) and perceived efficacy in past reasoned-based behavior (mediation effect = 0.050, BC 95%; CI = [0.010, 0.099]). The results confirmed the existence of a positive and negative mediation effect for perceived threat in defensive avoidance (mediation effect = −0.121, BC 95%; CI = [−0.202, −0.059]) and perceived efficacy in defensive avoidance (mediation effect = −0.109, BC 95%; CI = [−0.182, −0.058]). We also calculate the standard error (SE), critical ratios, and percentile-based bootstrap CI for these effects. These results support the CM assumption (indirect effect) in H1-a, H1-b, H2-a, H2-b, H3-a, and H3-b. Furthermore, the correlation coefficients indicated that habitual automatic behavior (r = .342, p < 0.001) and past frequent use (r = .542, p < 0.001) have a positively and significantly direct effect on future use intention, while defensive avoidance (r = −.285, p < 0.001) have a negatively and significantly direct effect on future use intention.

2.1.3 Author's Contribution to Article I

Yitian Xie proposed the research idea of the cognitive mediation mechanism in behavioral information security studies, analyzed the data, and wrote and revised the manuscript. Mikko Siponen participates in the conceptualization of the instrument, supervised the whole study, and revise the manuscript, and was responsible for funding acquisition. Gregory Moody was responsible for resources, software, and data curation. Xiao-song Zheng participates in the conceptualization of the instrument, and project administration.

2.2 Article II: Discovering the Interplay Between Defensive Avoidance and Continued Use Intention of Anti-malware Software Among Experienced Home Users: A Moderated Mediation Model

Xie, Y., Siponen, M., Moody, G., & Zheng, X. (2022). Discovering the interplay between defensive avoidance and continued use intention of anti-malware software among experienced home users: A moderated mediation model. *Information & Management*, 59(2), 103586.

2.2.1 Methods of Article II

To investigate the moderated mediation mechanisms, we first performed a mediation analysis. We applied a percentile-based bootstrapping confidence interval (CI) and a bias-corrected bootstrapping CI with 5,000 iterations to examine whether the mediation effects were present (Hayes, 2015, 2018).

To assess the significance of the moderated mediation effect, we performed an analysis using the user-defined syntax in AMOS 24.0 (Arbuckle, 2013). In this model, continued use intention (CONT) was entered as the outcome variable, defensive avoidance (DA) as the independent variable, and PE and PT as parallel mediators. Perceived vulnerability (VUL) and user involvement (UI) were included as two separated moderators on the dependent variables. Following Preacher et al.'s (2007) recommendation, we operationalized high and low levels of VUL (and UI) as one standard deviation above and below the mean score of VUL (and UI).

2.2.2 Results of Article II

As shown in Figure 1, the results confirmed the existence of a negative and significant mediation effect for perceived threat [−0.121 (95% CI = −0.202, −0.059)] and perceived efficacy [−0.109 (95% CI = −0.182, −0.058)] between defensive avoidance and continued use intention of anti-malware software. In addition, the results confirmed the existence of a positive and significant mediation effect for perceived efficacy [0.077 (95% CI = 0.040, 0.180)] between perceived threat and continued use intention of anti-malware software.

For VUL, the results show that the conditional indirect effects of DA had a positive influence and were significant in the VUL (VUL = 0.966, $p < 0.01$). In terms of user involvement, the results show that the conditional indirect effects of DA had a positive influence and were significant in the UI (UI = 0.993, $p < 0.01$).

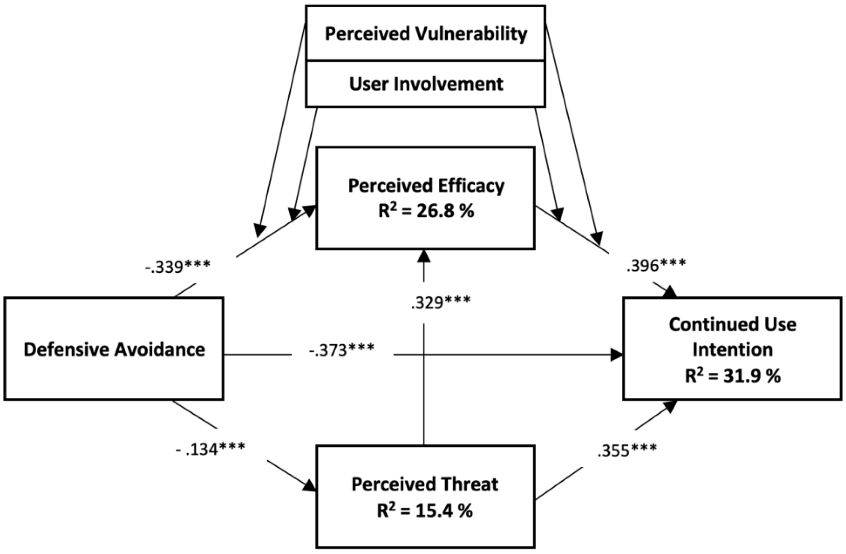


FIGURE 1 Model results

2.2.3 Author's Contribution to Article II

Yitian Xie proposed the moderated mediation model of the cognitive mediation process among defensively motivated home users, analyzed the data, and wrote and revised the manuscript. Mikko Siponen participates in the conceptualization of the instrument, supervised the whole study, and revise the manuscript, and was responsible for funding acquisition. Gregory Moody was responsible for resources, software, and data curation. Xiao-song Zheng participates in the conceptualization of the instrument, review & editing, and project administration.

2.3 Article III: Declarative and Procedural Information Security Knowledge of the General Public: Conceptualization and Instrument Development

Xie, Y., & Siponen, M (2022). Declarative and procedural information security knowledge of the general public: Conceptualization and instrument development. Unpublished manuscript.

2.3.1 Methods of Article III

In this section, we report on the instrument development process for the infosec knowledge of the general public.

Step 1. Develop Construct Definition

Construct clarity is essential in any measurement (MacKenzie, 2003). Following the recommendation of MacKenzie et al. (2011) and Podsakoff et al. (2016), we first developed the primary conceptual definition of ISK. Combine technology threat avoidance theory (TTAT, Liang & Xue, 2009) and two InfoSec behavior tendencies (i.e., approach and avoidance), we outlined a framework of ISK of personal users in Table 4.

TABLE 4 Framework of information security knowledge of personal users

	Approach tendency	**Avoidance tendency**
Declarative Knowledge (Factual information)	Component I Identify security tools/measures	Component II Identify cyber threats/risks
Procedural Knowledge (Cues- and situational- based *IF-THEN* Production)	Component III Cues- and situational- based security enhancement	Component IV Cues- and situational- based risk avoidance

Component I. Declarative Knowledge of Security Instrument (DK-S)

Declarative knowledge of security enhancement is factual knowledge of security tools or measures. It refers to people's awareness of the effectiveness and necessity of taking certain measures to ensure information security. For example, people know the fact that security software can protect email security. Or individuals know that two-factor authentication (2FA) is an identity protection tool.

Component II. Declarative Knowledge of ISec Risk (DK-R)

Declarative knowledge of risk avoidance is factual knowledge of cyber threats or risks. It refers to people's understanding of the possible risky situations related to the potential loss of information security assets. For example, people know that the relatively weak wireless network protection in public networks (e.g., at an airport, restaurant, or hotel) is unsafe. In addition, a man-in-the-middle attack may lead to personal information breaches in these public Wi-Fi environments.

Component III. Procedural Knowledge of Security Enhancement (PK-SE)

Procedural knowledge of security enhancement represents a decision-making production procedure in which people make security enhancement decisions based on infosec cues or situations. Two cognitive processes are involved in this procedure: (1) Individuals identify an infosec security cue or situation; (2) individuals adopt certain countermeasures (e.g., anti-malware tools) to enhance the information security of their computing environment based on certain cue or situational stimuli. By comprehensively assess the current situation and available tools, individuals practice security enhancement behavior to decrease the discrepancy between the current state and the desired security state. For instance, when there is an emergency need to process sensitive data via public Wi-Fi, people process the work duty via an alternative safe VPN. Or people know that keeping anti-malware software updated and active is an effective way to filter emails with virus software.

Component IV. Procedural Knowledge of Risk Avoidance (PK-RA)

Procedural knowledge of risk avoidance represents a decision-making production procedure in which people make risk avoidance decisions based on current infosec risk cues or situations. Two cognitive processes are involved in this procedure: (1) Individuals identify an infosec risk cue or situation; (2) individuals distancing or avoid the cyber threats or risks (e.g., been compromised by the cyber threats or risks) by action or no action based on certain cue or situational stimuli. By implementing a risk avoidance practice, individuals increase the discrepancy between the current state and the undesired insecurity state. For instance, when there is a need to use public Wi-Fi to process sensitive working data, people know that they are supposed to be aware there are potential cyber threats of hijacking, and they may delay this work duty until a secure connection is available. Just like we look around to see if an automobile is coming before we walk through a crosswalk, another example of risk avoidance behavior is that people are highly alert to their environment when they access or process sensitive information to avoid accidents that compromise their information security (e.g., shoulder-surfing). Other examples of these risk identifying and avoid behavioral pattern include when there is an email from strangers asking about sensitive information, or there is a phone call which needs us to state sensitive information out loud when we are in a public place (e.g., a café), individuals choose to consciously refuse those requirements.

Step 2. Measure Development

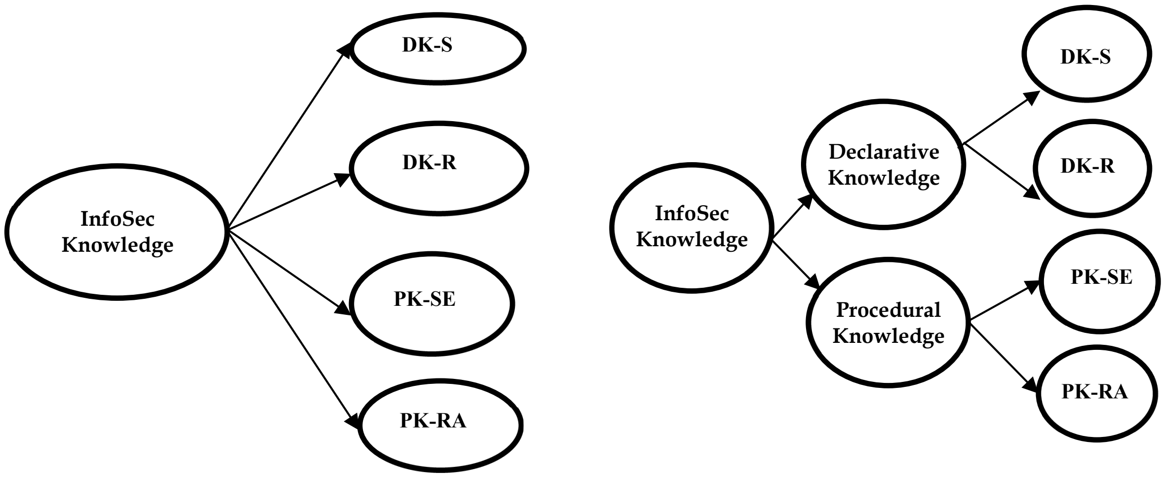
After determining the primary conceptual definition of ISK, we started the item generation process (DeVellis, 2016; Mackenzie et al., 2011). We investigated ten information security knowledge domains (see Appendix 1). They included password management (Bang et al., 2012; Grawemeyer, & Johnson, 2011), internet use (McElroy et al., 2007), Wi-Fi access (Consolvo et al., 2010), email use (Herath et al., 2014), social media use (Benson, 2015; Zhao and Zhao, 2015), identity theft (Berghel, 2002; Lai et al., 2012), electronics logistics (E-logistics) use (Tung et al., 2008), electronic health record (EHR) use (Burn et al., 2015; Fernández-Alemán et al., 2013), FinTech use (Lim et al., 2019), and mobile device security (Bitton et al., 2018; Imgraben et al., 2014; Markelj & Bernik, 2015; Mylonas et al., 2013a, 2013b). Based on these conceptual domains, we generated the initial item pool. According to the theoretical identification in Step 1, the item generation was based on the four conceptual components. In this step, we generated items based on four vectors: (1) security tool(s) or measure(s), (2) cyber threat or risk, (3) the cognitive decision process of security enhancement, and (4) the cognitive decision process of risk avoidance. The categorization of the ten information security domains is in Appendix 1.

Step 3. Assessment of the Content Validity of the Items

After creating the initial item pool, we assessed the content validity of the items (DeVellis, 2016; Mackenzie et al., 2011). Two researchers were asked to participate in the item screening process. The reviewers were asked to comment on the initial item pool with respect to (1) possible ambiguous, misleading, confusing, and wordy problems of the questions; (2) the conceptual deficiency and contamination of the questions; and (3) suggestions for improving and justifying each item. After the review process, we modified the ambiguous and tautological items suggested by reviewers.

Step 4. Formally Specify the Measurement Model

In this step, we formally specified a measurement model based on the four conceptual constructs in Step 1 (DeVellis, 2016; Mackenzie et al., 2011) (see Figure 2). We identified the hierarchical relationship between the constructs and four sub-components with theoretical justification and testify its validation in the following steps.



a. The first-order conceptual model

b. The second-order conceptual model

FIGURE 2 Two proposed conceptual models of information security knowledge

Step 5. Conduct Pretest Data Collection

After the formal specification of the measurement model, we conducted a pretest of the survey instrument (DeVellis, 2016; Mackenzie et al., 2011). The survey has two sections, which include the information sheet and consent form (section 1) and the main questionnaire (section 2). Information sheets and consent forms were signed by participants before they answered the formal questionnaire. The time for completing the questionnaire was around 15 to 25 minutes. We conducted a pretest among a small sample (n = 38) and reworded items that participants reported as confusing. After the pilot test of the instrument, we conducted three-waves of data collection to test and purify the instrument. The demographic data of the participant in the three-waves of data collection are reported in Table 5.

TABLE 5 Demographic data of the participants

	Sample I (n=233)		**Sample II** (n=281)		**Sample III** (n=289)	
	n	%	*n*	%	*n*	%
Gender						
Male	81	34.08	100	35.06	102	35.29
Female	152	65.02	181	64.04	187	64.70
Age						
18-22	115	49.04	136	48.04	98	33.91
23-27	59	25.03	75	26.07	102	35.29
28-32	7	3.00	11	3.09	25	8.65
33-37	4	1.07	5	1.08	8	2.77
38-42	48	20.06	54	19.02	56	19.38
Education						
Bachelor	179	76.08	214	76.02	118	40.83
Master	47	20.02	58	20.06	160	55.36
Ph.D.	7	3.00	9	3.02	11	3.81

Step 6. Scale Purification and Refinement

Following Mackenzie et al. (2011), we conducted scale purification and refinement after the pretest, and then we collected the first wave of data[1] (n = 233) with the original item pool (with 116 items). An online survey was used to collect data, all surveys were distributed with a simple random technique. After the first wave of data collection, we performed an item analysis (Ferketich, 1991; Siri & Freddano, 2011) which included (1) the independent sample t-test between the high-score group and the low-score group and (2) item-total correlation.

We conducted an independent sample t-test according to the following procedure to examine the discriminant validity of the items among our sample (Cohen, 2013). First, we encoded all the items in the scale and calculated the total score for each participant. Second, we sequenced the total score from the highest score to the lowest score and grouped the top 27% of the total score as the high-score group and the lowest 27% as the low-score group. Third, we performed an independent samples t-test with the low-score group and the high-score group and deleted the items with non-statistically significant t-test results, which show

[1] We applied three waves of data collection and item analysis in this study (Churchill, 1979). To avoid potential contamination of samples of different data collection waves (Benson & Clark, 1982), we informed the participants not to repeatedly participate in the future investigation of this study to ensure independent samples in different study phases. All three waves of data were collected from four universities in Shanghai, China. Appendix shows the demographic characteristics of the participants.

insufficient discriminant validity. The results for the independent sample t-test of the first-wave study are reported in Table 6.

We then calculate the item-total correlation to examine how well the responses to one item correlate with the other items in the scale. According to the psychometric criterion, the correlation between an item and a total score should be at least higher than 0.4 (Little 2013). Following this criterion, we deleted the items in which the correlation coefficient was lower than 0.4 among the initial item pool (with 116 items). After the first wave item analysis, 77 items remained. The results for the item-total correlation of the first wave study are reported in Table 7.

TABLE 6 Independent sample t-test of the first-wave study (n=233)

Item	*r*	Item	*r*	Item	*r*	Item	*r*
1	.323**	31	.717**	61	.721**	91	.450**
2	-.002	32	.407**	62	.705**	92	.543**
3	.385**	33	.685**	63	.709**	93	.487**
4	.253**	34	.709**	64	.381**	94	.453**
5	.310**	35	.411**	65	.625**	95	.538**
6	.189**	36	.634**	66	.359**	96	.527**
7	.553**	37	.389**	67	.579**	97	.595**
8	.402**	38	.425**	68	.728**	98	.372**
9	.327**	39	.620**	69	.073	99	.571**
10	.548**	40	.589**	70	.544**	100	-.311**
11	.510**	41	.698**	71	.466**	101	.511**
12	.407**	42	.702**	72	.217**	102	.517**
13	.620**	43	.361**	73	.084	103	.548**
14	.574**	44	.696**	74	.356**	104	.293**
15	.383**	45	.743**	75	.478**	105	.513**
16	.400**	46	.384**	76	.391**	106	.506**
17	.305**	47	.265**	77	.314**	107	-.200**
18	.513**	48	.707**	78	.462**	108	.326**
19	.356**	49	.719**	79	.501**	109	.619**
20	.584**	50	.348**	80	-.306**	110	-.419**
21	.628**	51	.669*	81	.509**	111	.537**
22	.390**	52	.601**	82	.426**	112	.566**
23	.524**	53	.616**	83	.456**	113	.465**
24	.404**	54	.032	84	.265**	114	-.350**
25	.265**	55	.507**	85	.445**	115	.509**
26	.617**	56	.532**	86	-.412**	116	.340**
27	.304**	57	-.023	87	.425**		
28	.639**	58	.727**	88	.517**		
29	.685**	59	.677**	89	.479**		
30	.722**	60	.666**	90	.524**		

** p < 0.01; * p < 0.05

TABLE 7 Item-total correlation of the first-wave study (n=233)

Item	*p*	Item	*p*	Item	*p*	Item	*p*
1	.000	31	.000	61	.000	91	.000
2	.724	32	.000	62	.000	92	.000
3	.000	33	.000	63	.000	93	.000
4	.000	34	.000	64	.000	94	.000
5	.000	35	.000	65	.000	95	.000
6	.013	36	.000	66	.000	96	.000
7	.000	37	.000	67	.000	97	.000
8	.000	38	.000	68	.000	98	.000
9	.000	39	.000	69	.480	99	.000
10	.000	40	.000	70	.000	100	.000
11	.000	41	.000	71	.000	101	.000
12	.000	42	.000	72	.000	102	.000
13	.000	43	.000	73	.166	103	.000
14	.000	44	.000	74	.000	104	.000
15	.000	45	.000	75	.000	105	.000
16	.000	46	.000	76	.000	106	.000
17	.000	47	.000	77	.000	107	.000
18	.000	48	.000	78	.000	108	.000
19	.000	49	.000	79	.000	109	.000
20	.000	50	.000	80	.000	110	.000
21	.000	51	.000	81	.000	111	.000
22	.000	52	.000	82	.000	112	.000
23	.000	53	.000	83	.000	113	.000
24	.000	54	.823	84	.000	114	.000
25	.000	55	.000	85	.000	115	.000
26	.000	56	.000	86	.000	116	.000
27	.000	57	.697	87	.000		
28	.000	58	.000	88	.000		
29	.000	59	.000	89	.000		
30	.000	60	.000	90	.000		

** p < 0.01; * p < 0.05

Step 7. Conduct New Sample Data Collection

To purify and refine the scale, we conducted the second wave of data collection. A total of 281 usable responses were collected. The aim of the second wave was to assess the retest reliability and the validation of the multidimensional construct of the concept (Straub et al., 2004) of the scale. We recruited new participants who had not participated in the first wave of data collection. The same item analysis (Ferketich, 1991; Siri & Freddano, 2011) was applied to examine the second wave of data, which included 1) the independent sample t-test between the high-score group and the low-score group (Cohen, 2013) and 2) item-total correlation (Little, 2013).

The results for the independent sample t-test of the second-wave study are reported in Table 8. The results for the item-total correlation of the second-wave study are reported in Table 9. After this purification procedure, 52 items were retained.

TABLE 8 Independent sample t-test of the second-wave study (n=281)

Item	*r*	Item	*r*	Item	*r*	Item	*r*
7	.653**	34	.764**	61	.801**	92	.558**
8	.374**	35	.462**	62	.746**	93	.495**
10	.637**	36	.689**	63	.775**	94	.488**
11	.581**	38	.417**	65	.680**	95	.560**
12	.347**	39	.686**	67	.604**	96	.538**
13	.700**	40	.653**	68	.786**	97	.581**
14	.658**	41	.755**	70	.595**	99	.620**
16	.458**	42	.782**	71	.497**	101	.528**
18	.602**	44	.722**	75	.534**	102	.571**
20	.682**	45	.743**	78	.474**	103	.616**
21	.727**	48	.755**	79	.558**	105	.512**
23	.595**	49	.772**	81	.550**	106	.579**
24	.465**	51	.696*	82	.432**	109	.640**
26	.684**	52	.614**	83	.490**	111	.544**
28	.700**	53	.670**	85	.460**	112	.573**
29	.754**	55	.505**	87	.444**	113	.552**
30	.802**	56	.546**	88	.526**	115	.498**
31	.812**	58	.765**	89	.515**		
32	.373**	59	.725**	90	.635**		
33	.699**	60	.692**	91	.456**		

** $p < 0.01$; * $p < 0.05$

TABLE 9 Item-total correlation of the second-wave study (n=281)

Item	*p*	Item	*p*	Item	*p*	Item	*p*
7	.000	34	.000	61	.276	92	.000
8	.179	35	.109	62	.000	93	.000
10	.000	36	.000	63	.000	94	.000
11	.007	38	.101	65	.000	95	.000
12	.108	39	.000	67	.690	96	.000
13	.000	40	.134	68	.675	97	.000
14	.000	41	.016	70	.637	99	.000
16	.298	42	.008	71	.000	101	.000
18	.000	44	.171	75	.000	102	.000
20	.000	45	.193	78	.000	103	.000
21	.000	48	.000	79	.000	105	.000
23	.189	49	.008	81	.311	106	.000
24	.803	51	.000	82	.064	109	.000
26	.477	52	.000	83	.264	111	.000
28	.000	53	.000	85	.000	112	.000
29	.000	55	.905	87	.000	113	.000
30	.000	56	.276	88	.217	115	.000
31	.000	58	.000	89	.000		
32	.628	59	.000	90	.384		
33	.000	60	.000	91	.000		

** $p < 0.01$; * $p < 0.05$

Step 8. Cross-validation

To test the stability of the scale, we collected data from a new sample (n = 289), the demographic data are shown in Table 5. We performed the item analysis (Ferketich, 1991; Siri & Freddano, 2011) which included 1) the independent sample t-test between the high-score group and the low-score group (Cohen, 2013) and 2) item-total correlation (Little, 2013). The results for the independent sample t-test of the third-wave study are reported in Table 10. The results for the item-total correlation of the third-wave study are reported in Table 11. The results for the third wave of item analysis showed satisfied discriminant validity and homogeneity of the scale. After this procedure, 52 items were retained.

Next, we calculated the Cronbach alpha coefficient and the Pearson correlation of the sub-scale and the full scale with the new sample. As shown in Table 12, the Cronbach alpha coefficient of the full scale was 0.797, and the internal consistency coefficient of each factor (F1–F4) was between 0.656 and 0.801, which indicates good reliability. Table 12 shows the correlation matrix of each component and the full scale. The relatively low correlation among the four sub-scales indicates good discriminant validity.

TABLE 10 Independent sample t-test of the third-wave study (n=289)

Item	*r*	Item	*r*	Item	*r*	Item	*r*
7	.549**	34	.693**	65	.745**	96	.474**
10	.543**	36	.718**	71	.497**	97	.472**
11	.618**	39	.687**	75	.503**	99	.490**
13	.559**	48	.716**	78	.539**	101	.557**
14	.572**	49	.718**	79	.518**	102	.485**
18	.523**	51	.668*	85	.497**	103	.486**
20	.686**	52	.569**	87	.589**	105	.482**
21	.719**	53	.678**	89	.569**	106	.401**
28	.665**	58	.733**	91	.400**	109	.583**
29	.687**	59	.715**	92	.578**	111	.457**
30	.698**	60	.702**	93	.483**	112	.568**
31	.716**	62	.696**	94	.581**	113	.539**
33	.709**	63	.698**	95	.519**	115	.588**

** p < 0.01; * p < 0.05

TABLE 11 Item-total correlation of the third-wave study (n=289)

Item	*p*	Item	*p*	Item	*p*	Item	*p*
7	.000	34	.000	65	.000	96	.000
10	.000	36	.000	71	.000	97	.000
11	.000	39	.000	75	.000	99	.000
13	.000	48	.000	78	.000	101	.000
14	.000	49	.000	79	.000	102	.000
18	.000	51	.000	85	.000	103	.000
20	.000	52	.000	87	.000	105	.000
21	.000	53	.000	89	.000	106	.000
28	.000	58	.000	91	.000	109	.000
29	.000	59	.000	92	.000	111	.000
30	.000	60	.000	93	.000	112	.000
31	.000	62	.000	94	.000	113	.000
33	.000	63	.000	95	.000	115	.000

** p < 0.01; * p < 0.05

TABLE 12 Cronbach α and correlation matrix of the sub-constructs

Dimension	**Cronbach α**	**F1**	**F2**	**F3**	**F4**	**Total Score**
F1	.656	1				
F2	.746	.755**	1			
F3	.799	.496**	.392**	1		
F4	.801	.421**	.351**	.582**	1	
Full Scale	.797	.930**	.840**	.682**	.642**	1

Step 9. Assess the Multi-dimensionality of the Scale

To identify the multi-dimensionality of the latent constructs (Edward et al., 2001; Law et al., 1998; Little, 2013), we conducted an exploratory factor analysis (EFA) and confirmation factor analysis (CFA) with the retained 52 items. Bartlett's test of sphericity (x2 (377) = 0.675, p < 0.000) showed that our data were correlated and measured common factors. Moreover, according to the Kaiser criterion (i.e., retain eigenvalues > 1.0), the result shows that there are four components been retained (see Table 13). After the EFA, we tested the hierarchical relationship between the first- and second-order constructs identified in Step 4. In this step, we specifically inspected the following psychometric indexes:

1. the item loadings for the reflectively measured first-order and second-order constructs;
2. goodness-of-fit of the model;
3. the unique proportion of variance that each first-order construct explained in the associated second-order construct;
4. the reliability of the full- and sub-scale.

As shown in the results, all item loadings of the first-order constructs are ranged between 0.523 and 0.782, all the item loadings for the reflective indicators of the second-order construct were above 0.7, which is acceptable for an exploratory study (Hair et al., 2006). We tested the model fit of the overall model and heuristically using several goodness-of-fit statistics to assess the quality of the CFA model. The chi-square statistic ($\chi2$/df) was 1.739, which is below the cutoff value suggested by Hair et al. (2006). The root mean square error of approximation (RMSEA) was 0.051, the standardized root mean square residual (SRMR) was 0.057, which is below the recommended cut-off points (Hu & Bentler, 1999). The comparative fit index (CFI) was 0.899, and the Tucker-Lewis index (TLI) was 0.981, which is in line with the recommended cutoff value (Netemeyer et al., 2003). As shown in the results (Table 14.), the Cronbach alpha coefficient of the full- and sub-scales are above the recommended cutoff value which shows good reliability. Moreover, the result shows that the first-order constructs explained a significant proportion of variance in the second-order constructs (see Table 15.). This result aligned with the previous theoretical assumptions and specifications in Step 4.

TABLE 13 Factor loading matrix

	Factor			
Item	F1	F2	F3	F4
53	.751			
52	.740			
62	.716			
58	.704			
65	.699			
39	.696			
60	.692			
49	.692			
48	.663			
51	.651			
63	.648			
34	.646			
31	.629			
59	.623			
33	.602			
36	.577			
10		.670		
14		.662		
20		.637		
7		.616		
13		.590		
18		.579		
11		.556		
21		.523		
96			.761	
115			.730	
97			.684	
112			.645	
91				.782
79				.736
105				.696
101				.624

TABLE 14 Cronbach α, eigenvalues, and the accumulate variance explained by the first-order factor

Dimension	**Cronbach α**	**F1**	**F2**	**F3**	**F4**	**Total Score**
F1	.656	1				
F2	.746	.755**	1			
F3	.799	.496**	.392**	1		
F4	.801	.421**	.351**	.582**	1	
Full Scale	.797	.930**	.840**	.682**	.642**	1

TABLE 15 Eigenvalues and the accumulate variance explained by the second-order factor

Second-order Factor	Eigenvalue	Variance explained	Accumulate variance explained
F1	1.745	43.641	43.641
F2	1.605	40.115	83.756

Step 10. Norm Development

The final step was to develop norms for the new scale (MacKenzie et al., 2011). The scale was collected from students and staff at four universities in Shanghai. Each data collection phase followed the independent data collection procedure, and all participants were informed not to repeatedly answer the survey. In total, we surveyed 1045 individuals. The population was relatively young (age: 18–42 years). This sample frame (age group) was supposed to represent the millennial population with relatively higher IT literacy and more experience of using digital technology and service among the general public.

2.3.2 Results of Article III

In this section, we report the statistical results of the developed instrument for infosec knowledge of the general public (see Appendix). The results showed a second-factor conceptual model that consisted of two second-order factors: declarative knowledge and procedural knowledge; and four first-order factors: declarative security enhancement knowledge, declarative risk avoidance knowledge, procedural security enhancement knowledge, and procedural risk avoidance knowledge. Next, we specify the structure and meaning of the constructs.

Component I. Declarative Knowledge of Security Instrument (DK-S)

This sub-scale (sub-construct) includes 16 questions that mainly involve information security enhancement facts or tools, such as two-factor authentication, wireless network security standard (WPA2/WPA3-PSK), ad-blocking tools, and so on. This factor contains the four focus areas, including the security of household mobile devices, identity theft, internet use, Wi-Fi access, data backup, password management, and FinTech use. The variance explained by this factor was 22.934%.

Component II. Declarative Knowledge of ISec Risk (DK-R)

This sub-scale (sub-construct) includes eight items that are mainly related to people’s understanding of information security risks: security incidents and potential threats, such as identity theft illicit by a phishing email, a man-in-the-middle attack via public Wi-Fi, and inappropriate disposal of sensitive documents. This factor contains areas such as identity theft, email use, Wi-Fi access, and FinTech use. The variance explained by this factor was 10.923%.

Component III. Procedural Knowledge of Security Enhancement (PK-SE)

This sub-scale (sub-construct) includes four items that relate to how individuals take security measures (or use security tools, such as software, firewalls, complex passwords, etc.) to enhance the security of the computing environment according to different circumstances. The variance explained by this factor was 9.671%.

Component IV. Procedural Knowledge of Risk Avoidance (PK-RA)

This sub-scale (sub-construct) includes four items that relate to how individuals identify and avoid information security risk with certain measures. There are three topics: email use, Wi-Fi access, and internet use. The variance explained by this factor was 8.775%.

2.3.3 Author's Contribution to Article III

Yitian Xie proposed the research idea of the concept decomposition of ISK and the instrument development of the sub-area of ISK; was responsible for data collection; analyzed the data and wrote and revised the manuscript. Mikko Siponen participated in the conceptualization of the sub-area of ISK, the methodology discussion of instrument development, supervised the whole study and revise the manuscript, and was responsible for funding acquisition.

3 DISCUSSION OF THE KEY FINDINGS

In this dissertation, we make contributions not only to the theorizing process and empirical validation but also by reconsidering the methodological merit[2] of moderation, mediation, and conceptual refinement in the process of contextualization.

The following five conclusions, in particular, can be drawn from the findings of Article I, which compared the three motivation-driven prospective models of the continued use of anti-malware among experienced home users. First, previous adaptive coping behavior (including automatic habitual behavior and past reason-based behavior) can directly increase home users' continued intention to use anti-malware. These results are aligned with previous empirical findings (e.g., Kim, Malhotra, and Narasimhan, 2005).

Second, defensive avoidance can directly decrease home users' continued intention to use anti-malware. This finding is in line with the results of a meta-analysis regarding the relationship between defensive avoidance and health-conducive behaviors (Witte and Allen, 2000). Interestingly, the perception of threat and efficacy can both mediate the relationship between the antecedent of adaptive and maladaptive coping and continued intention to use anti-malware and act as a facilitator to help home users in the appraisal and reappraisal process and facilitate their continued intention to use anti-malware. This finding further supports Rogers' (1985) notion that the CMs are key in the message acceptance of threat information.

Third, comparison of the CM effects of the three proposed models shows that perceived threat and perceived efficacy have the strongest effects on the antecedent of defensive avoidance. A possible explanation of this result is that more cognitive efforts are needed for protection intention formation with the antecedent of defensive reaction. Moreover, the analysis of the multiple mediation model allows us to zoom in on the relationship between IVs and DVs. The results of the multiple mediation analysis show that automatic behavior and defensive reaction are higher than reason-based behavior. Since both automatic

[2] Moderation, mediation, and refinement of constructs have been regarded as three "methodologically equivalent" tools of the exploration of boundary conditions (Busse, Kach & Wagner, 2017).

behavior and defensive reaction are behavioral coping with less consciousness involved, this may explain why CMs counted more in protection intention formation with automatic antecedents.

Fourth, Article I also gives empirical evidence of how users' experience may influence their continued use intentions. Specifically, users with longer anti-malware use experience show more cognitive appraisals of threat and efficacy. This result is intuitive because more experienced users tend to have a higher chance of interacting with different ISec threats and the threat-mitigating process. This result implies that ISec practitioners should consider this factor in their future design of security communication messages to promote more effective anti-malware use.

Fifth, Article I also offers insights into the usage of automatic features among home users. Specifically, home users tend to perceive a higher efficacy of anti-malware protection after enabling the automatic function. Our study results offer suggestions to ISec practitioners that encourage home users to enable some automatic features in their daily computer use which may improve their efficacy perception of anti-malware protection for their home computers.

Article II explores the cognitive mediation and decision-making process of security-related behavior of experienced home users. Whereas most classic fear appeal theories have proposed that defensive motivation will result in security-impairing behaviors or undermine persuasion in some other way (e.g., Witte 1994, Witte and Allen, 2000), the perspective provided by Article II suggests that defensively motivated individuals may process information in a biased way. The result of the moderated mediation model in the study offers empirical evidence for another theoretical perspective that is distinct from classic fear appeal theories.

The results highlight two boundary conditions (perceived vulnerability and user involvement) that may influence the security-related decision-making of defensively motivated users. The effect of the moderation role of perceived vulnerability is in line with the stage model's assumption that defensive motivation does not always undermine persuasion but can sometimes enhance it when individuals perceive themselves to be vulnerable to a highly relevant threat. Article II also sheds light on the similar effect of the moderation role of user involvement on security-related decision-making of expedited home users.

These study results offer guidance to both researchers and practitioners. Consider that a home computer can be accessed by multiple family members, each of whom may perceive varying levels of user involvement (or, say, psychological relevance) and vulnerability to certain malware threats. Thus, practitioners should consider depicting and stressing the vulnerability, psychological significance, and personal relevance of the negative consequences of malware threats to various family members. In so doing, they can encourage home users to engage in more active use of anti-malware software on their home computers.

Article III makes contributions to the information security field by decomposing and conceptualizing ISK as four sub-constructs: knowledge of declarative infosec tool(s), declarative infosec risk knowledge, procedural infosec knowledge, and procedural infosec risk knowledge. While most previous ISec studies use ISK as a generic term, Article III distinguishes these four constructs with the aim of more precisely defining each to facilitate future related studies. Future researchers could thus have a more precise conceptual understanding of ISK. Moreover, by offering this definition, researchers and practitioners can identify these four vectors and conduct more relevant studies and offer guidance to future information security education, training, and awareness (SETA) programs. In addition, Article III provides preliminary evidence for a hierarchical relationship among the sub-constructs of ISK.

Lastly, Article III contributes to the behavioral ISec study by outlining an infosec knowledge measurement instrument (ISK-DP), which can be used for future instrument development and validation as well as SETA practice.

In addition, this dissertation illustrates three methodology tools to explore the boundary condition of theory, which may not only act as amendments of theory but also facilitate theoretical development. Moreover, exploring the boundary condition can be helpful in diminishing the gap between research and practice (Busse, Kach & Wagner, 2017). First, the explanation of the boundary conditions (e.g., mediation) allows us to give a more accurate and detailed interpretation of the model and facilitates the comparison of the empirical results. In Article I, we highlight the importance of cognitive mediation, not only as a statistical tool but also as a theoretical assumption, which can facilitate a clearer delineation of theoretical representation and the comparison of empirical results in the context of ISec research. Second, the process of contextualization (e.g., moderation) helps researchers to identify potential enhancements or modifications of our understanding regarding a phenomenon of interest.

In Article II, drawing on SMFAC, we explore the boundary condition of household anti-malware use intention among experienced home users. Specifically, the study results provide a nuanced delineation by empirically testing two boundary conditions (perceived vulnerability and user involvement) in security communication and offer detailed guidance to security communication practitioners. Third, the exploration of boundary conditions (e.g., refinement of construct) gives us better insight into the potential theoretical and practical application of the research with the refinement of the contextual factors in the real world.

In Article III, drawing on TTAT and the knowledge categorization model, we decompose the generic concept of ISK to a more refined definition and empirically test the second-order model with 1045 participants. In addition, we develop and preliminarily test the reliability and validity of the instrument. The refinement of the ISK can be helpful for future theory validation and instrument development.

4 CONCLUSIONS

This dissertation addresses the influence of cognitive appraisals, emotional motivation, user characteristics, and ISec knowledge of personal users by focusing on three studies that explore the security-related decision-making process. By using novel theoretical perspectives and revisiting the "old" theoretical assumptions, we offer insights of value to both academics and practitioners. Three studies are tested and reported that provide insights respectively for the cognitive appraisals, emotional motivation, user characteristics, and ISec knowledge of personal users' decision-making process of security-related behavior.

By considering additional theories and constructs and revisiting the theoretical and methodology perspectives, this dissertation provides several contributions to behavioral information security studies. The results of the empirical study provide new insights into the cognitive mediation process, decision-making process under the influence of defensive avoidance, and personal users' self-regulated ability to secure their information and personal computing devices.

4.1 Conclusions of Article I

Previous ISec research has underutilized the CM mechanism in threat-based theories. Three underutilization situations are typical: (1) no mediation assumption and test; (2) underestimation of the theoretical cues of "partial mediation"; and (3) neglect of the theoretical and methodological merits of multi-mediation analyses. In this paper, this gap was addressed by the reintroduction of the theoretical origins and the method applied in the threat-based theories. Furthermore, for illustration purposes, we empirically tested three mediation models to measure the continued use of anti-malware among home users. The results confirmed that the CM mechanism theorized with the original assumptions; that is, prior coping (the IV)–cognitive appraisal (M)–cognitive outcome (the DV).

Our findings suggest the following:

1. Cognitive appraisals of threat severity and response efficacy can be initiated by three antecedent motivation-driven constructs (including automatic habitual use, reasoned-based use, and defensive avoidance).
2. The three-antecedent motivation-driven constructs could directly influence home-users' continued use intention of anti-malware software.
3. The cognitive appraisal process can indirectly mediated prior automatic habitual use and reasoned-based use and can change prior defensive avoidance. The CM effects of perceived threat and perceived efficacy have the strongest effects with the antecedent of defensive avoidance.
4. Users with longer anti-malware use experience show more reflective cognitive appraisals of the threat and efficacy.
5. After enabling automatic function, home users perceived a higher efficacy of anti-malware protection.

4.2 Conclusions of Article II

While an unbiased or accuracy-motivated individual assesses personal relevant information in an information-based manner, the processing goal of defense-motivated individuals is to confirm the validity of a preferred position and process information in a biased way. Our study findings demonstrate that defense-motivated individuals will process and perceive information in ways that may help conserve cognitive resources and eliminate emotional distress. Our study provides a starting point for integrating the moderation role of the perceived vulnerability and user involvement in the information-processing perspective of fear-eliciting persuasion in household anti-malware use among experienced users.

4.3 Conclusions of Article III

This paper focused on the unaddressed research gap in the conceptualization and measurement of the multi-dimension characteristics of ISK of the general public. We conducted a three-wave study to develop an instrument to test ISK, and preliminarily test the second-order hierarchical relationships of ISK. The empirical results showed the multi-dimensional characteristics of information security knowledge. For declarative knowledge, users know what security tool(s) or measure(s) they should take, and what potential risks may exist in different information security scenario(s). For procedural knowledge, the user(s) "know-how" to adopt security tool(s) to enhance the security of the computing environment(s) and keep distances from potential infosec risks. Furthermore, this study contributes to infosec studies by offering a measurement tool for declarative and procedural infosec knowledge.

YHTEENVETO (SUMMARY IN FINNISH)

Tässä väitöskirjassa omaksumme erilaisia teoreettisia näkökulmia, validoimme niitä empiirisesti ja tarkastelemme uudelleen medioinnin, moderoinnin ja käsitteellisen tarkentamisen metodologisia ansioita teorian kontekstualisointiprosessissa. Teorialainauksen ja empiirisen validoinnin osalta otamme erilaisia teorianäkökulmia terveyspsykologiasta ja muilta aloilta. Testaamme niitä empiirisesti henkilökohtaisen tietoturvakäyttäytymisen kontekstissa.

Väitöskirja sisältää kolme artikkelia. Artikkelissa I tarkastelemme kognitiivisen välitysmekanismin teoreettista alkuperää pelon vetovoimateorioissa, otamme uudelleen käyttöön useita vaikutuskokomittareita monivälitysanalyysiin ja esittelemme teoreettisen selityksen ja tilastollisen analyysin empiirisen tutkimuksen kera. Pelkoa herättävän viestinnän vaihemalliin perustuvassa artikkelissa II oletetaan, että tapa, jolla ihmiset käsittelevät pelkoa herättävää viestiä, määräytyy heidän käsittelymotivaationsa perusteella. Tulokset viittaavat siihen, että tiedot, jotka lisäävät käyttäjien suurta osallistumista tai saavat yksilön tuntemaan olevansa haavoittuvaisia itselleen merkitykselliselle ei-triviaalille uhalle, saavat todennäköisesti aikaan puolueellisen kognitiivisen arviointiprosessin. Artikkelissa III luokittelemme tietoturvatiedon neljään luokkaan perustuen teknologiauhkien välttämisteoriaan ja tietokategorioiden erotteluun. Lisäksi testaamme empiirisesti tietoturvatiedon neljän osarakenteen hierarkkista suhdetta ja kehitämme instrumentin henkilökohtaisten käyttäjien tietoturvatiedon mittaamiseen.

Väitöskirjassa tarkastellaan uudelleen medioinnin, maltillisuuden ja käsitteellisen tarkentamisen metodologisia ansioita teorian kontekstualisointiprosessissa. Kolmessa artikkelissa käsitellään useita näkökohtia, joihin aikaisemmassa käyttäytymiseen liittyvässä tietojärjestelmien turvallisuuden tutkimuksessa on kiinnitetty vain vähän huomiota huolimatta siitä, että muilla aloilla niitä on laajalti käsitelty tai raportoitu (esim. useiden välitysanalyysien metodologiset ansiot). Väitämme, että parempi teoreettinen kehitys ja teorian validointi voidaan saavuttaa tarkastelemalla perusteellisemmin tutkimuksen tavoitteen, epistemologisen lähestymistavan ja tutkimusmenetelmien yhteensopivuutta. Jos se lisää medioinnin, moderoinnin ja käsitteellisen tarkentamisen metodologisten ansioiden uudelleen tarkastelemista tutkimuksemme valaisemassa teorian kontekstualisointiprosessissa, väitöskirja täyttää hyödyllisen tarkoituksensa.

REFERENCES

Anderson. C. L. & Agarwal. R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613. https://doi.org/10.2307/25750694

Aurigemma, S. & Mattson, T. (2019a). 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). https://doi.org/10.17705/1jais.00583

Aurigemma, S. & Mattson, T. (2019b). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security*, *73*, 219-234

Aurigemma, S.,Mattson, T., & Leonard, L. (2019). Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications, *AIS Transactions on Replication Research*. *5*(3). https://doi.org/10.17705/1atrr.00035

Bamberger, P. (2008). From the editors: Beyond contextualization: Using context theories to narrow the micro–macro gap in management research, *The Academy of Management Journal*, *5* (51), 839-846 https://doi.org/10.5465/amj.2008.34789630

Baron, R. M., & Kenny, D. A. (1986). *The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations*. 10.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Bowins, B. (2004). Psychological Defense Mechanisms: A New Perspective. *The American Journal of Psychoanalysis*, *64*(1), 1–26. https://doi.org/10.1023/B:TAJP.0000017989.72521.26

Brown, S., & Locker, E. (2009). Defensive responses to an emotive anti-alcohol message. *Psychology & Health*, *24*(5), 517–528. https://doi.org/10.1080/08870440801911130

Busse C., Kach A. P., & Wagner S. M. (2017). Boundary Conditions: What They Are, How to Explore Them, Why We Need Them, and When to Consider Them. *Organizational Research Methods*, *20*(4), 574-609. https://doi:10.1177/1094428116641191

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. *Information Systems Research*.

Chen, Y., Zahedi, F. M., & Milwaukee. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, *40*(1), 205–222. https://doi.org/10.25300/MISQ/2016/40.1.09

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: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Das, E. H. H. J., de Wit, J. B. F., & Stroebe, W. (2003). Fear Appeals Motivate Acceptance of Action Recommendations: Evidence for a Positive Bias in the Processing of Persuasive Messages. *Personality and Social Psychology Bulletin*, *29*(5), 650–664. https://doi.org/10.1177/0146167203029005009

Davison, RM., & Martinsons, MG. (2015). Context is king! Considering particularism in research design and reporting. *Journal of Informaion Technology*, 31 (3), 241-249. https://doi.org/10.1057/jit.2015.19

de Hoog, N., Stroebe, W., & de Wit, J. B. F. (2005). The Impact of Fear Appeals on Processing and Acceptance of Action Recommendations. *Personality and Social Psychology Bulletin*, *31*(1), 24–33. https://doi.org/10.1177/0146167204271321

de Hoog, N., Stroebe, W., & de Wit, J. B. F. (2007). The Impact of Vulnerability to and Severity of a Health Risk on Processing and Acceptance of Fear-Arousing Communications: A Meta-Analysis. *Review of General Psychology*, *11*(3), 258–285. https://doi.org/10.1037/1089-2680.11.3.258

de Hoog, N., Stroebe, W., & de Wit, J. B. F. (2008). The processing of fear-arousing communications: How biased processing leads to persuasion. *Social Influence*, *3*(2), 84–113. https://doi.org/10.1080/15534510802185836

Haag, S., Liu, F., Siponen, M. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM Database* 52(2): 25-67.

Hansen, J., Winzeler, S., & Topolinski, S. (2010). When the death makes you smoke: A terror management perspective on the effectiveness of cigarette on-pack warnings. *Journal of Experimental Social Psychology*, *46*(1), 226–228. https://doi.org/10.1016/j.jesp.2009.09.007

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

Hong, W., Chan., Thong., Chasalow., & Dhillon G. (2014). A Framework and Guidelines for Context Specific Theorizing in Information Systems Research. *Information Systems Research*, *23*(2), 111–136. https://doi.org/10.1287/isre.2013.0501

Hovav, A. (2017). How espoused culture influences misuse intention: a micro-institutional theory perspective. *Procedings of the 50th Hawaii International Conference on System Sciences.*

Hovav, A, & D'arcy, J. (2012). Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. *Information & Management*. *49*(2), 99-110

Johnston & Warkentin. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549. https://doi.org/10.2307/25750691

Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems, *25*(3), 231–251. https://doi.org/10.1057/ejis.2015.15

Karjalainen, M., Siponen, M. Puhakainen P, Sarker S (2013). One size does not fit all: different cultures require different information security interventions. Paper presented at the PACIS; 2013.

Karjalainen, M., Siponen, M. & Sarker, S. (2019). Towards a Theory of Information Systems security Behaviors of Organizational Employees: A dialectical Perspective. *Information Systems Research*, *30*(2), 351-710.

Karjalainen, M., Siponen, M., Sarker, S. 2020. Toward A Stage Theory of the Development of Employees' Information Systems Security Behavior. *Computers & Security*, *93*(June), 101782.

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), pp. 435-453.

Li, H., Luo, X. R., & Chen, Y. (2021). Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems*, *22*(3), 5.

Ying, L. Tong, X, Siponen, M. 2022. Citizens’ Cybersecurity Behavior: Some Major Challenges. *IEEE Security & Privacy*, forthcoming

Liang, H., & Xue, Y., (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33*(1), 71. https://doi.org/10.2307/20650279

Liang, H., & Xue, Y., (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(07), 394–413. https://doi.org/10.17705/1jais.00232

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.

Luo, X. R., Li, H., Hu, Q., & Xu, H. (2020). Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective. *Journal of the Association for Information Systems*, *21*(6), 5.

MacKinnon, D. P. (2008). *Introduction to statistical mediation analysis*. Lawrence Erlbaum Associates.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, T. (2009). What Levels of Moral Reasoning and Values Explain Adherence to Information Security Policies? An Empirical Study. *European Journal of Information Systems 18*(2): 126–139.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1–20. https://doi.org/10.1057/s41303-016-0025-y

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 156b–156b. https://doi.org/10.1109/HICSS.2007.206

Preacher, K. J. (2015). Advances in Mediation Analysis: A Survey and Synthesis of New Developments. *Annual Review of Psychology*, *66*(1), 825–852. https://doi.org/10.1146/annurev-psych-010814-015258

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Posey, C., Roberts, T. L., Lowry, P. B., & Bennett, R. (2013). Insiders' protection of organization of organizational information assets: Developing of a systematic-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*(4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778. https://doi.org/10.2307/25750704

Putri, F. F., & Hovav, A. (2014). Employees' Compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. *Twenty Second European Conference on Information Systems*.

Richiardi, L., Bellocco, R., & Zugna, D. (2013). Mediation analysis in epidemiology: Methods, interpretation, and bias. *International Journal of Epidemiology*, *42*(5), 1511–1519. https://doi.org/10.1093/ije/dyt127

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 psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychophysiology: A sourcebook*, 153-176. Guilford Press.

Siponen, M.T. (2001): On the Role of Human Morality in Information System Security: From the Problems of Descriptivism to Non-Descriptive Foundations. *Information Resource Management Journal*, Special Issue on Social Responsibility, Vol. 14, No. 4, 2001, pp. 15-23.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. von Solms (Eds.), *New Approaches for Security, Privacy and Trust in Complex Environments* (Vol. 232, pp. 133–144). Springer US. https://doi.org/10.1007/978-0-387-72367-9_12

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. *2006 Innovations in Information Technology*, 1–5. https://doi.org/10.1109/INNOVATIONS.2006.301907

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *IEEE Computer Society*, *43*(2), 64–71. http://doi.org/10.1109/MC.2010.35

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Siponen, M. & Baskerville, R. (2018). Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. *Journal of the Association for Information Systems* 19(4), 247-265.

Siponen, M. & Klaavuniemi, T. 2020. Why Is the Hypothetico-Deductive (H-D) Method in Information Systems Not an H-D Method. *Information and Organizations*, 30(1).

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2013). Managing the introduction of information security awareness programs in organizations. *European Journal of Information Systems*, *24*(1), 38–58. https://doi.org/10.1057/ejis.2013.27

van 't Riet, J., & Ruiter, R. A. C. (2013). Defensive reactions to health-promoting information: An overview and implications for future research. *Health Psychology Review*, *7*(sup1), S104–S136. https://doi.org/10.1080/17437199.2011.606782

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

Vance, T., Siponen, M., Straub, D., 2020. The Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures. *Information & Management*, *57* (4).

VanderWeele, T. J. (2016). Mediation Analysis: A Practitioner's Guide. *Annual Review of Public Health*, *37*(1), 17–32. https://doi.org/10.1146/annurev-publhealth-032315-021402

VanderWeele, T., & Vansteelandt, S. (2014). Mediation Analysis with Multiple Mediators. *Epidemiologic Methods*, *2*(1). https://doi.org/10.1515/em-2012-0010

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860-870.

Warkentin, M., Straub, D. and Malimage, K. (2012). Featured talk: measuring secure behavior: a research commentary, *Annual Symposium of Information Assurance and Secure Knowledge Management*, Albany, New York, NY.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study.

Decision Support Systems, *92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Xin, T., Siponen, M. & Chen, S (2021) Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats, Behaviour & Information Technology, DOI: 10.1080/0144929X.2021.1954242

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. *Journal of Consumer Research*, *37*(2), 197–206. https://doi.org/10.1086/651257

ORIGINAL PAPERS

I

THE COGNITIVE MEDIATION PROCESS IN THREAT-BASED THEORIES IN IS SECURITY

by

Yitian Xie, Mikko Siponen, Greg Moody and Xiaosong Zheng (2022)

Submitted to *Computers & Security*

Request a copy from author.

II

DISCOVERING THE INTERPLAY BETWEEN DEFENSIVE AVOIDANCE AND CONTINUED USE INTENTION OF ANTI-MALWARE SOFTWARE AMONG EXPERIENCED HOME USERS: A MODERATED MEDIATION MODEL

by

Yitian Xie, Mikko Siponen, Greg Moody and Xiaosong Zheng (2022)

Information & Management, 59(2), 103586

https://doi.org/10.1016/j.im.2021.103586

Information & Management 59 (2022) 103586

Contents lists available at ScienceDirect

Information & Management

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

Discovering the interplay between defensive avoidance and continued use intention of anti-malware software among experienced home users: A moderated mediation model

Yitian Xie [a], Mikko Siponen [a], Greg Moody [b], Xiaosong Zheng [c,*]

[a] University of Jyvaskyla, Finland
[b] University of Nevada, United States
[c] Shanghai University, China

ARTICLE INFO

Keywords:
Stage model of fear-arousing communication processing (SMFAC)
Defensive avoidance
User involvement
Moderated mediation
Experienced user

ABSTRACT

Dismissing or disregarding security notifications (defensive avoidance) may lead to inactive use of anti-malware, compromising the effective protection of home computers. Nevertheless, few studies have investigated the cognitive and behavioral mechanisms initiated by defensive avoidance in users. Motivated thus, we propose a moderated mediation model that depicts users' cognitive and behavioral mechanisms initiated by defensive avoidance, as well as the moderation role of perceived vulnerability and user involvement. Our results show that perceived vulnerability and user involvement may moderate a biased cognitive mediation process between defensive avoidance and future behavioral intention.

1. Introduction

The mushrooming growth of Internet connectivity has made billions of home computers potential targets for malware. Malware can cause a plethora of issues for home users, such as the loss of personal data, credit card numbers, and passwords, as well as decreased computer speed for applications [1]. Malware threats can be effectively averted by employing anti-malware software in an active way (e.g., performing scans regularly or updating the software) [62]. However, some home users engage in defensive avoidance by, for example, having a behavioral tendency to dismiss or disregard security notifications by the anti-malware software. We refer to this type of defensive avoidance as passive use of anti-malware software. Use of defensive avoidance as a cognitive and behavioral regulation strategy can effectively attenuate negative emotions and preserve cognitive resources, and thus, it can facilitate effective functioning of daily life [8]. Previous studies in psychology suggest that defensive avoidance is usually triggered by emotion-elicit and self-relevant stimuli with a high degree of immediacy [7, 60, 65]. In the context of household anti-malware use, users with defensive motivation tend to divert attention away from security notifications with a cognitive and behavioral regulation strategy (i.e., defensive avoidance). Although defensive avoidance might help to lessen disturbing emotion and conserve cognitive resources, it can also make anti-malware software less efficient at protecting home computers and devices. While it appears that defensive avoidance may act as an inhibitor to individual intention to engage in intensive and thoughtful message processing, it is unclear how defensiveness tendencies affect cognitive appraisals of the severity of malware threat, the effectiveness of anti-malware software, and intentions to actively use anti-malware software. Specifically, previous studies suggest that high perceived vulnerability may influence the cognitive mediation process among defensively motivated individuals (e.g., [18]). In addition, previous studies suggest that user involvement, which implies perceived consequent relevance and psychological significance, may also alter the cognitive mediation process in response to some self-relevant threats (e.g., [14]; Gleicher & Petty, 1992). In summary, there is a paucity of research on users who exhibit defensive reactions, thereby necessitating further scientific investigation.

According to the stage model of fear-arousing communication processing (SMFAC), there are two cognitive appraisal processes in fear appeal: threat appraisal and efficacy appraisal [18]. Threat appraisal emphasizes the perceived severity of a threat and the perceived vulnerability to a threat. Efficacy appraisal indicates individuals' evaluations of the effectiveness of the action recommendation. Moreover,

[*] Corresponding author.
E-mail addresses: yixie@student.jyu.fi (Y. Xie), mikko.t.siponen@jyu.fi (M. Siponen), greg.moody@gmail.com (G. Moody), xiaosong.zheng@shu.edu.cn (X. Zheng).

https://doi.org/10.1016/j.im.2021.103586
Received 1 November 2019; Received in revised form 21 December 2021; Accepted 23 December 2021
Available online 25 December 2021

there are, among defensive-motivated individuals, two distinct information processing methods: (a) defensive avoidance that may act as an inhibitor of the intention to engage in intensive and thoughtful message processing and (b) cognitively or behaviorally regulated strategies that may result in biased cognitive appraisals [18–20]. In addition, based on the dual-process theories of attitude change (Gleicher & Petty, 1992; [55]), fear-arousal can have two different effects. It can motivate intensive (and accurate) message processing, or it can generate defensively motivated (biased) message processing. While defensive motivation may be aroused when self-definitional beliefs are threatened (e.g., when the belief that "my household computing environment is safe" is in conflict with a security notification of a severe and personal relevant threat), there is a paucity of research on how defensive motivation may influence users' intentions to proactively use anti-malware software. Therefore, we propose the first research question:

> **RQ1(1)**: *How does defensive avoidance influence users' cognitive appraisals and their subsequent behavioral intention to actively use anti-malware on their home computer(s)*?
> **RQ1(2):** *Do users with defensive avoidance tendencies process threat information in a suppressive or biased way*?

According to the SMFAC, individuals who perceive higher vulnerability to threats exhibit more negative emotions toward threats, a more favorable evaluation of action recommendations, and a stronger willingness to react to action recommendations [18]. Moreover, SMFAC suggests that in those who are defensively motivated, perceived vulnerability may attenuate a biased cognitive evaluation process. Specifically, defensively motivated individuals who perceive a higher level of vulnerability to a certain threat may selectively process information in ways that best support their own beliefs, allowing them to maintain emotional homeostasis and conserve cognitive resources. Therefore, we propose the second research question:

> **RQ2**: *How does perceived vulnerability moderate the relationship between defensive avoidance and user's continued use intention of anti-malware software in their home computer(s)*?

Many prior studies in psychology have found that individuals who are highly relevant to specific threats may act in a defensive way (e.g., avoidance, denial) in response to the threat information [9–11, 44, 45]. In the context of household anti-malware software use, home users with high user involvement (e.g., those who perceive the malware attack as having more personal relevance to themselves than to other family members) may downplay the severity of malware threats from security notifications as well as the effectiveness of anti-malware protection more than individuals with low user involvement. Therefore, we propose the third research question:

> **RQ3**: *How does user involvement moderate the relationship between defensive avoidance and users' future intentions to actively use anti-malware software in their home computer(s)*?

In essence, we posit (RQ1–RQ3) that defensive avoidance towards security notifications can impede the effectiveness of anti-malware software protection on home computers. To advance this line of research, our study addresses this issue by closely investigating how defensive-motivated users process security messages and when these cognitive appraisals are heightened because of two personal relevance characteristics (e.g., perceived vulnerability and user involvement). We collected data from experienced users who have installed anti-malware software on their home computers. This study contributes to the Information Systems (IS) security literature by theoretically proposing and empirically testing a moderated mediation model in the context of household anti-malware software use among experienced users, and this study extends the current IS security studies (e.g., [41, 42]) by offering a perspective beyond classic fear appeal theories that assume that information processing initiated by threatening messages is subject to an objective and information-based calculation. In particular, by answering RQ1–RQ3, we attempt to discover and contribute the cognitive appraisals and behavioral intentions of individuals who have a defensive motivation. Departing from pertaining empirical research in health psychology [18–20], by studying RQ2, we discover that defensive-motivated individuals have a positive-biased belief in the effectiveness of countermeasures and a negative-biased belief in the severity of threats. Further, we find that this cognitive bias processing will only occur when people perceive high vulnerability towards malware threats. In addition, by studying RQ3, we find that user involvement aggravates this cognitive-biased processing. Practitioners might also gain from this study a better understanding of the interplay between the information processing mechanism of security notifications and defensive motivations (e.g., users with high vs. low perceived vulnerability; users with high vs. low user involvement towards the malware threats).

In the next section, we introduce the theoretical background of the proposed research model. In the third section, we elaborate on the research hypotheses based on the theoretical background. In the fourth section, we introduce the data collection, analytic method, and results. In the fifth section, we discuss the key findings, theoretical implications, practical implications, and limitations of this study. In the last section, we make conclusions for this study.

2. Theoretical background

In this section, we establish the theoretical foundations for our original work by introducing the SMFAC [18–20], defensive avoidance [74, 75], the moderation roles of perceived vulnerability [18], and user involvement [31].

2.1. A stage model of the processing of fear-arousing communication

SMFAC [18–20] illustrates how people process fear-arousing information. It assumes that the way in which people process a fear-arousing message is determined by their processing motivation and that, in accordance with cognitive stress theories [49], individuals exposed to fear-arousing communication will engage in two types of appraisals in sequence: an appraisal of the threat and an appraisal of the coping strategies available for reducing the threat. Individuals processing a fear-arousing message first evaluate the severity of, and their vulnerability to, a malware threat (primary appraisal) and then evaluate the effectiveness of the action recommendation, which provides information on how to avoid the malware threat (secondary appraisal). SMFAC [18–20] suggests that information that makes an individual feel vulnerable to a nontrivial threat (e.g., malware's compromise of their home computer) is likely to induce a negative processing bias in the primary appraisal process (i.e., the severity of the malware threat) and a positive processing bias in the secondary appraisal process (i.e., the efficacy of the protection action). The negative bias entails a skewed evaluation of the presented fear appeal communication (e.g., the severity of a malware threat depicted in a security notification). The positive bias involves an overly positive belief in the effectiveness of the existing countermeasures (e.g., the protection of an installed anti-malware software). Previous empirical studies in health psychology show that this biased cognitive appraisal processing occurs only when individuals perceive high vulnerability [18–20].

2.2. Defensive avoidance

Psychological defense mechanisms represent a crucial component of our capacity to maintain emotional homeostasis and serve an important function by attenuating negative emotions to maintain or restore a healthier state of mind ([8, 44]; Kessels et al., 2011). Defensive avoidance is commonly regarded as an unconscious reaction that is elicited automatically by self-relevant emotional stimuli [7, 60]. Defensive avoidance evolves in humans due to its ability to attenuate negative emotions and thus maintain or restore a state of mind conducive to effective functioning and self-regulation [8]. The most important proximal goal for people with defensive motivation is to maintain a neutral or positive emotional state rather than to achieve objectively optimal solutions [25, 48]. Individuals will be motivated to use defensive strategies to the extent that those strategies make them feel good, rather than to the extent that the strategies improve problem-solving [71]. This is because defensive strategies are most effective at inhibiting negative emotions immediately in order to facilitate emotional homeostasis. Previous studies suggest that defensive reactions to health-promoting information do not always reduce health-conducive responses but can co-occur with or even facilitate more adaptive responses (e.g., [71]).

2.3. The moderation role of perceived vulnerability

Previous studies have illustrated the impact of vulnerability to and severity of a threat on the processing of both the fear appeal information and the subsequent action recommendation (e.g., [18–20]). Building on the assumptions of dual-process theories of attitude change (Chaiken, 1980), the stage model predicts the impact of the perceived severity and perceived vulnerability on people's information processing motivation and information processing mode [18]. The stage model depicts a situation in which individuals feel vulnerable to a severe threat that seriously threatens self-definitional beliefs about their safety and, as a result, may arouse defensive motivation. Defense motivation induced by the perception of a threat as severe should manifest itself not only in avoidance reactions, as previous fear appeal models have proposed (e.g., [74]), but also in biased systematic processing [14]. Stage models indicate that vulnerability to a severe health risk induces defense motivation, as evidenced by a cognitive bias in the processing of the fear appeal [18].

2.4. The moderation role of user involvement

User involvement refers to the degree to which an object has personal relevance, psychological significance, and significant consequences for an individual [4, 31]. Previous studies indicate that individuals with higher user involvement (e.g., perceived higher financial cost if personal computers are compromised as a result of a malware attack) tend to perceive certain systems as more useful and relevant to their work performance [31, 35]. Previous research suggests that threatening messages with a higher personal relevance tend to increase defensive or self-protective behavior toward a certain message (e.g., [47, 55]). In line with cognitive dissonance theory [25], previous studies posit that when users perceive they are at risk of certain threats (high perceived vulnerability), higher personal involvement may prompt them to engage in more biased, defensive processing toward threatening stimuli than toward non-threatening stimuli [13]. According to Liberman and Chaiken ([55], p. 669), "with non-threatening messages, increased personal relevance will often increase motivation to arrive at an accurate conclusion ... but with a threatening message, increased personal relevance may instead increase motivation to arrive at or defend a preferred conclusion or reject an undesirable one". To investigate the information processing method of defensive-motivated users, we will focus in this study on the moderation role of user involvement on the cognitive appraisal process that is initiated by defensive avoidance.

3. Hypothesis development

Experienced users may perceive inconvenience when security notifications request immediate actions to eliminate certain malware threats via a fear-inducing message (i.e., security notifications). These messages may contradict beliefs related to their current state and elicit a defensive motivation. To alleviate feelings of discomfort, defensive-motivated users are likely to employ cognitive and behavioral regulation strategies (e.g., defensive avoidance) to counteract the dissonance caused by personal relevant threats [71, 74, 75]. Defensive avoidance is commonly regarded as an unconscious reaction that is elicited automatically by self-relevant emotional stimuli [7, 60]. To alleviate distress, defensive-motivated users tend to shift their attention away from threatening stimuli [12, 15]. In the context of household anti-malware use, defensive-motivated users may tend to minimize and dismiss the severity of the threats portrayed in security notifications. Thus, we hypothesize that:

Hypothesis 1: Defensive avoidance negatively influences perceived severity of a malware threat.

Experienced users of anti-malware may experience discomfort when receiving security notifications (e.g., frightening warnings about a new malware threat) that contradict their beliefs related to the efficacy appraisal of anti-malware (e.g., I believe my computing devices are safe; [12, 15]). While people are aware of the inconsistency between their beliefs and the action recommendation, they intend to alleviate their discomfort through cognitive or behavioral strategies (e.g., defensive avoidance; [25, 43]). People with a defensive disposition tend to shift their attention away from evaluating the effectiveness of countermeasures in order to conserve cognitive resources or relieve discomfort feelings, especially because defensive avoidance requires fewer efforts than does a behavioral coping response [71, 74, 75]. In the context of household anti-malware software use, experienced users with defensive avoidance motivation tend to downplay the efficacy of anti-malware software protection because they believe that their computers are adequately protected. Therefore, they tend to perceive the protection of anti-malware software as less effective in order to remain consistent with their existing beliefs. Thus, we hypothesize that:

Hypothesis 2: Defensive avoidance negatively influences the perceived efficacy of current anti-malware protection.

Previous empirical studies have also found that defensive avoidance is negatively associated with precautionary behavior [76]. Defensive avoidance constitutes the guidance of attention away from threatening stimuli. Defensive-motivated users tend to disengage from actively using anti-malware software because a fear appeal message (e.g., security notification) contains preference-inconsistent information [25, 43]. This avoidance reaction results in weaker and less elaborate memory representations of threatening stimuli, as well as less trust in the protection provided by anti-malware software. Furthermore, defensive avoidance may also reduce later accessibility of threat stimuli [29] and lower belief in the malware threat and in the effectiveness of anti-malware software protection [71]. This may impede users' subsequent intention to actively use anti-malware software. Thus, we hypothesize that:

Hypothesis 3: Defensive avoidance negatively influences future use intention to actively use household anti-malware software.

Perceive efficacy refers to the degree to which an individual believes a recommended response will effectively avert a threat [63, 74]. Appraisal of response efficacy is a cognitive process through which individuals form thoughts about the effectiveness of a recommended response's ability to avert a threat [74]. Ultimately, it is their beliefs of response efficacy that determine how they respond to the threat (Rogers, 1983). According to protection motivation theory (PMT; [63, 64]), response efficacy is associated with positive feelings toward the threat mitigation through which a recommended response is enacted. Users tend to form a disposition toward the future behavioral intention to actively use anti-malware software through the evaluation and confirmation of the capabilities of anti-malware software protection. Thus, we hypothesize that:

Hypothesis 4: Perceived efficacy positively influences future use intention to actively use household anti-malware software.

Perceived severity of the threat refers to an individual's belief regarding the seriousness of a certain threat [63, 74]. Previous studies suggest a positive correlation between the perceptions of threat severity and the continued intention to conduct security actions (e.g., [41, 72]). Perceived severity of the threat is a necessary condition to continued engagement in certain protective security behaviors, especially when the threat is perceived to be personally relevant (Rogers, 1983). Alternatively, if there is a lack of perceived significant threat, it is possible that previous protective security behaviors (e.g., anti-malware software use) may cease. Thus, we hypothesize:

Hypothesis 5: Perceived severity of threat positively influences future use intention to actively use household anti-malware software.

In the context of household anti-malware software use among experienced users, variations in the perceived severity of the malware threat can cause users to reassess the effectiveness of anti-malware protection during their usage of anti-malware software. During the continued use of certain security technology, post-adoptive belief regarding the efficacy of security technology protection will increase as a function of the perception of severity of the malware threats (Vedadi & Warkentin, 2020). In other words, users' beliefs regarding the protective capability of certain security technology tend to increase in strength once the users perceive that a related information technology (IT) security threat is significant ([51, 52]; Vedadi & Warkentin, 2020). Because of the rarity of security incidents, users may perceive anti-malware software as more effective when the malware threat is perceived as more severe. On the other hand, users may perceive anti-malware software as less effective when the malware threat is perceived as not serious. Based on this argument, we hypothesize:

Hypothesis 6: Perceived severity of malware positively influences the perceived efficacy of household anti-malware software.

An effective defensive reaction will usually lead to message rejection [74, 75]. Specifically, people with a defensive avoidance inclination might devalue the protection effectiveness of their current use of anti-malware software. Furthermore, the belittled appraisal of anti-malware efficacy will negatively influence users' future use intention toward their household anti-malware software [19, 22]. Therefore, disparaging appraisals of the efficacy of anti-malware protection tend to negatively mediate both users' previous defensive inclination and their future intention to actively use anti-malware software. Thus, we hypothesize:

Hypothesis 7-a: Perceived efficacy mediates the relationship between defensive avoidance and future intention to actively use household anti-malware software.

Defensive avoidance may dilute the perception or cognitive representation of the severity of the threat ([44]; Kessels et al., 2011). This cognitive and behavioral regulation strategy impedes the intention to be aware of and manage objective dangers or threats [74, 75]. Moreover, minimized evaluation of the severity of a malware threat leads to diminished intention to actively participate in future protective behavior. Therefore, the appraisal of the severity of the malware under defensive avoidance motivation will negatively mediate the relationship between defensive avoidance inclination and users' future use intention toward their household anti-malware software. Thus, we hypothesize:

Hypothesis 7-b: Perceived severity of threat mediates the relationship between defensive avoidance and future intention to actively use household anti-malware software.

According to SMFAC, experienced users tend to first reevaluate the severity of malware threats and then reevaluate the effectiveness of anti-malware protection [18–20]. Previous studies suggest that the perceived severity of the threat, as the primary component of cognitive appraisal, will positively influence the user's perception of the efficacy of the use of anti-malware software [42, 72]. The effectiveness of anti-malware protection is manifest with the increasing perceived severity of malware threats. Perceived efficacy, as the second component of cognitive appraisal, will also positively influence the user's intention to continue actively using anti-malware software [42, 72]. Therefore, a positive evaluation of the efficacy of currently utilized anti-malware software will positively mediate the perceived severity of malware threat and future use intention. Thus, we hypothesize:

Hypothesis 7-c: Perceived efficacy mediates the relationship between perceived severity of threat and future intention to actively use household anti-malware software.

Perceived vulnerability refers to individuals' perceived susceptibility to a threat and perceived inability to withstand the harmful effects of a threat [63, 74]. During the use of anti-malware software, variations in perceived vulnerability will affect individuals' coping responses toward the security recommendation. When they perceive lower vulnerability to certain threats, users are more likely to process recommendations in a systematic and objective manner. However, users who perceive higher vulnerability to malware threats tend to be more defensively motivated, resulting in the processing of information in a heuristic and biased way [18–20]. An increase in perceived vulnerability will increase heuristic and biased information processing among defensive-motivated users. Specifically, they tend to hold a positive bias toward the recommended security actions while also holding a negative bias toward the severity of malware threats [18–20]. Thus, negative emotions evoked by perceived vulnerability to malware threats directly moderate the cognitive appraisals process by which users process the security notification. Therefore, we posit that:

Hypothesis 8: Perceived vulnerability moderates the strength of the mediation relationships between defensive avoidance and continued use intention via perceived efficacy, such that the mediated relationship will be stronger in the high perceived vulnerability group than in the low perceived vulnerability group.

User involvement refers to individuals' subjective evaluations of the importance and personal relevance of a system to themselves [4, 31]. Previous studies suggest that individuals with high user involvement may process self-relevant threat information in a biased way [13, 55]. In the context of household anti-malware use, anti-malware notifications may arouse more cognitive dissonance for users who perceive higher user involvement (i.e., higher personal relevance regarding potential damage caused by the malware threats). To counteract this cognitive dissonance and achieve a stable emotional state, they tend to process information in a heuristic and biased way that is consistent with their preferent beliefs. Specifically, these users tend to process information in a biased way that rates the threat as less severe and the countermeasure as more effective. This biased information processing may lead to a future intention to actively use anti-malware software in their home computer. Therefore, we hypothesize:

Hypothesis 9: User involvement moderates the strength of the mediation relationships between defensive avoidance and continued use intention via perceived efficacy, such that the mediated relationship will be stronger for high involvement users than for low involvement users.

In light of the SMFAC, this study proposes a theoretical model that assumes that the continued use intention may be influenced by both heuristic and biased information processing and by a systematic, information-based calculation based on threat and coping appraisals (see Fig. 1). In addition, we tested the moderation role of two context-specific factors in the household context in order to obtain a more refined understanding of how and when information processing may influence the continued use intention among defensively motivated users.

4. Data and methods

4.1. Data collection

The data were collected from a Qualtrics, LLC panel of 502 adults from the United States. Qualtrics is a market and survey method firm that provides a panel of qualified survey respondents and has been widely used in previous IS security studies (e.g., Barlow et al., 2013, 2018; Menard et al., 2018). Qualtrics did not disclose information on the total number of individuals who initiated the survey, and we only received the responses of those who anonymously completed it. We

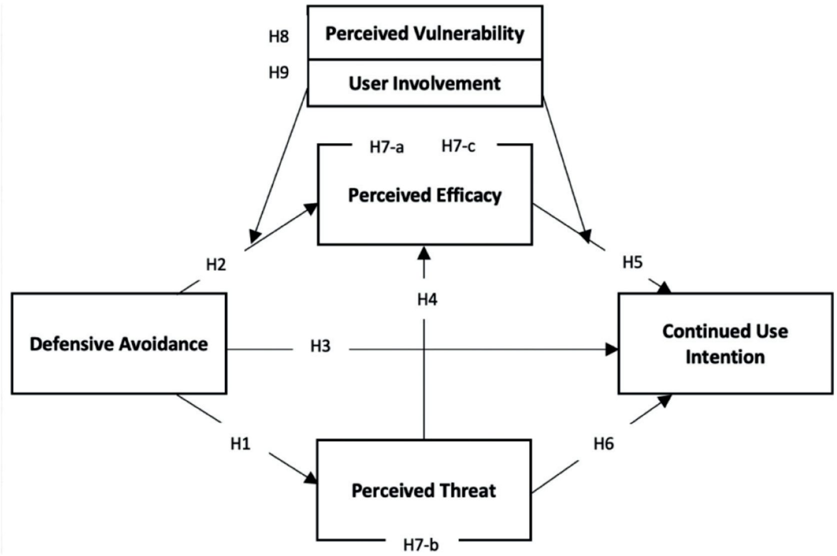


Fig. 1. The Proposed Research Model

recruited full-time employees who had used anti-malware software on their home computer for at least six months. Participants took an online survey (www. Qualtrics.com) that was used to investigate individuals' perceptions of home information security and their intentions to actively use anti-malware software on their home computer(s). Appendix 1 presents the constructs and measurement items in this study.

4.2. Sample characteristics

All the participants had used anti-malware software on their home computer(s) for more than a year. Details of the respondents' demographic information are shown in Table 1. The sample size (n = 502) was sufficient for testing the covariance-based structural equation model with the maximum likelihood (ML) algorithm [36] to detect the mediation effect [26] and the moderated mediation effects [61, 68]. In addition, we performed a power analysis to test for sample size using Rweb1.03 [69]. The result showed that our sample size provides adequate statistical power for the model.

4.3. Common-method variance

We conducted both procedural control and statistical remedies for potential common-method variance (CMV; [70]). For procedural control, we took the following proactive steps. First, we used anonymous statements in the survey instrument to reduce social desirability bias. Second, we counterbalanced the order of all the questions. Third, we used the attention checks techniques to make sure that the participants paid careful attention to their responses, such as "For this question only answer 2, agree; do not give any other answer." A marker variable technique [77] was also used to examine CMV. We considered using masculinity/femininity as the marker variable, and we compared the structural model with the marker variable and without it. No statistically significant correlation was found between the marker variable and the principal constructs in the model, and the path efficiencies were not altered when the marker variable was added. Therefore, CMV was not a serious caveat in our study.

Table 1
Demographics of Respondents

	N = 502	
Characteristic	Frequency	%
Gender		
Male	251	50
Female	251	50
Age		
18–30	59	12
31–40	81	16
41–50	108	22
51–60	141	28
Above 60	112	22
Not Reported	1	0
IT-related work		
IT-related	56	11
Non-IT-related	446	89

5. Results

In this research, we performed data analyses using SPSS 24.0 and AMOS 24.0[1] to examine the measurement and structural models. We choose covariance-based SEM rather than PLS because of the confirmatory rather than exploratory research objectives of this study [27].

5.1. Measurement model

Table 2 shows the loadings of the measures of our model as well as

Table 2
Chi-Square, Goodness-of-Fit Values, and Model Comparison Tests

Model	χ^2	df	CFI
CFA	173.905	104	0.988
Baseline	234.034	114	0.982
Method-U	198.971	100	0.982
Method-C	222.5	113	0.979
Method-R	698.843	105	0.980
Chi-square model comparison tests			
ΔModels	$\Delta\chi^2$	Δdf	Chi-Square critical value
Baseline vs. Method-C	35.063*	14	3.001
Method-C vs. Method-U	49.53*	13	9.036
Method-U vs. Method-R	23.872	5	7.830

* $p<0.05$. CFI: comparative fit index; CFA: confirmatory factor analysis.

[1] The moderated mediation analysis is estimated by user-defined syntax [3].

Table 4
Latent variable correlation

	AVE	DA	CONT	PE	PT	UI
DA	0.685	**0.828**				
CONT	0.901	–0.341	**0.949**			
PE	0.612	–0.046	0.267	**0.782**		
PT	0.546	–0.254	0.394	0.573	**0.739**	
UI	0.800	–0.134	0.543	0.144	0.120	**0.894**

Table 5
HTMT results

	UI	DA	CONT	PE	PT
UI	–				
DA	0.134	–			
CONT	0.543	0.342	–		
PE	0.144	0.046	0.267	–	
PT	0.120	0.255	0.396	0.575	–

descriptive statistics of the measures (mean, standard deviation, kurtosis, and skewness). We used Cronbach's alpha and composite reliability (CR) to assess internal consistency. Cronbach's alphas of our data ranged from 0.711 to 0.967, which exceeded the baseline of 0.7. The CRs in this study ranged from 0.776 to 0.965, exceeding the baseline of 0.7 and demonstrating the good internal consistency of our dataset. Next, the average variance extracted (AVE) values were used to test convergent validity. The AVE value for each construct was higher than 0.5 (see Table 3), which proves our scales' good convergent validity. Moreover, we checked the potential multicollinearity in our model. All variance inflation factors (VIF) in our model were below 2, indicating that multicollinearity was not an issue in our analyses.

Furthermore, we used the square root of the AVE values and latent variable correlations to evaluate discriminant validity. Good discriminant validity requires the AVE value's square root for each variable to be higher than the correlations between that and all other variables. Table 4 shows that our dataset has adequate discriminant validity. In addition, we conducted a further discriminant validity test using the heterotrait–monotrait (HTMT) ratio of correlations criteria [34]. The HTMT ratios presented in Table 4 are all under the threshold value of 0.85, demonstrating that our dataset did not suffer from discriminant validity problems.

5.2. *Structural model*

The covariance-based structural equation modeling followed the procedure suggested by Kline [46]. We performed a chi-square test on the measurement and structural models and heuristically used the goodness-of-fit index to evaluate the quality of the three models. The results show that both the measurement model ($\chi^2 = 78.825$ (67), $p = .153$) and the structural model ($\chi^2 = 35.776$ (38), $p = .573$) passed the chi-square test. Furthermore, the results of the goodness-of-fit index check show that all indicators achieved good model fit (see Table 5). All path coefficients achieved statistical significance in our model (see Fig. 2). Hence, the results show strong support for H1–H6. Table 6

5.3. *Moderation mediation model*

To investigate the moderated mediation mechanisms, we first performed a mediation analysis. We applied a percentile-based bootstrapping confidence interval (CI) and a bias-corrected bootstrapping CI with 5,000 iterations to examine whether the mediation effects were present [32, 33]. As shown in Figure 2, the results confirmed the existence of a negative and significant mediation effect for perceived threat [−0.121 (95% CI = −0.202, −0.059)] and perceived efficacy [−0.109 (95% CI = −0.182, −0.058)] between defensive avoidance and continued use intention of anti-malware software. These results support H7-a and H7-b. In addition, the results confirmed the existence of a positive and significant mediation effect for perceived efficacy [0.077 (95% CI = 0.040, 0.180)] between perceived threat and continued use intention of anti-malware software, thereby supporting H7-c.

To assess the significance of the moderated mediation effect, we performed an analysis using the user-defined syntax in AMOS 24.0 [3]. In this model, CONT was entered as the outcome variable, DA as the independent variable, and PE and PT as parallel mediators. VUL and UI were included as two separated moderators on the dependent variables. Following Preacher et al.'s [68] recommendation, we operationalized high and low levels of VUL (and UI) as one standard deviation above and below the mean score of VUL (and UI). For VUL, the results show that the conditional indirect effects of DA had a positive influence and were significant in the VUL (VUL = 0.966, $p < 0.01$). Thus, Hypothesis 8 was supported. In terms of user involvement, the results show that the conditional indirect effects of DA had a positive influence and were significant in the UI (UI = 0.993, $p < 0.01$). Thus, Hypothesis 9 was supported.

6. Discussion

6.1. *Key findings*

In this study, we examined the direct effect of defensive avoidance on cognitive appraisals and behavioral intention; the indirect effect of PE and PE between DA and CONT; the indirect effect of PE between PT and CONT; and two conditional effects of VUL and UI on the cognitive mediation process under a defensive avoidance motivation.

Table 3
Measurement model's reliability and validity

Variables	Items	Mean	SD	Factor loadings	Cronbach's alpha	CR	Skew	Kurtosis
Perceived threat (PT)	threat1	5.75	0.066	0.757	0.866	0.776	–0.338	–0.127
	threat2	4.8	0.079	0.534			–0.621	–0.607
	threat3	5.71	0.063	0.883			–0.675	0.405
Perceived efficacy (PE)	avoid1	5.74	0.052	0.868	0.931	0.867	–0.85	1.102
	avoid2	5.55	0.049	0.809			–0.775	0.776
	avoid3	5.84	0.049	0.804			–0.83	1.198
Continued use intention (CONT)	cont1	5.07	0.083	0.912	0.967	0.965	0.094	–0.487
	cont2	5.18	0.081	0.969			0.178	–0.639
	cont3	5.13	0.081	0.965			0.175	–0.707
Defensive avoidance (DA)	defavoid1	2.91	0.078	0.726	0.711	0.825	0.096	–1.144
	defavoid2	2.67	0.075	0.815			–0.016	–1.367
	defavoid3	2.9	0.073	0.802			–0.151	–0.782
User involvement (UI)	userinv1	5.18	0.081	0.899	0.953	0.923	0.4	–1.142
	userinv2	4.67	0.082	0.888			0.519	–0.866
	userinv3	5.08	0.081	0.896			0.585	–0.546
Multivariate							56.199	10.948

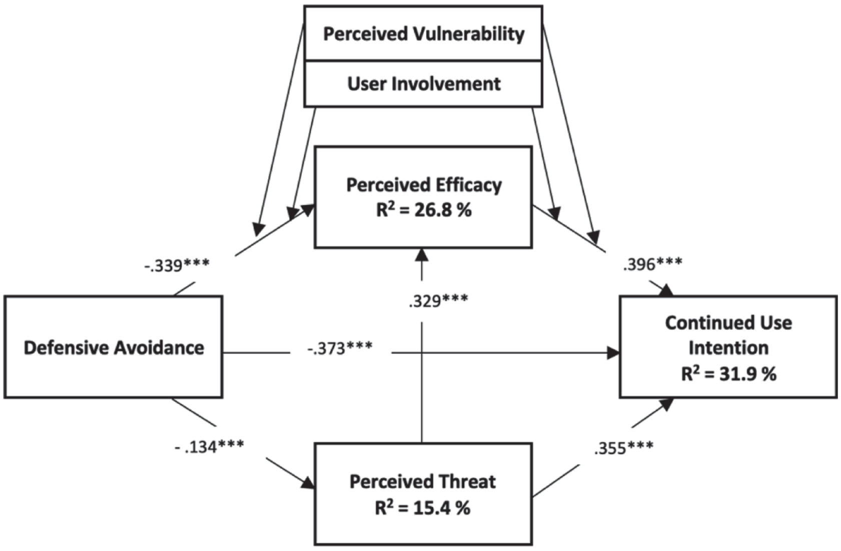


Fig. 2. Model Results

Table 6
Model Fit

Index		Measurement model	Structural model
χ^2		78.825	35.776
P	H_0: $\varepsilon_0 \leq 0.05$	0.153	0.573
Df	n–1	67	38
Fit index	Recommended value	Measurement model	Structural model
CFI	≥0.92	0.985	0.991
NFI	≥0.90	0.909	0.961
SRMR	≤0.05	0.034	0.042
RMSEA	≤0.08	0.051	0.000

We contribute to existing knowledge in the following ways. First, we found support for our hypothesis among the DA, PT, PE, and CONT (H1–H3). This finding supports previous studies by Witte [74, 75] on the cognitive and behavioral coping responses elicited by DA. We discovered that DA, a specific behavioral response construct based on a defensive motivation targeted at message processing, accounted for the mediation effects of PT and PE on CONT.

Second, we found support for our hypothesis between the DA, PT, PE, and CONT (H4 and H5). This finding supports previous studies of classic view of fear appeal theories (e.g., [63], 1983), which concern the impact of cognitive appraisal of threat and the effectiveness of countermeasures on protective behavioral intentions. In addition, the support for Hypothesis 6 indicates a positive relationship between PT and CONT via PE among experienced users.

Third, our mediation results support Hypotheses 7-a–c, which explain *how* defensive avoidance users process the fear-eliciting information (i.e., security notification) during the post-adoptive use of anti-malware software in their home computer. These results are consistent with the theoretical propositions in PMT ([63], 1983). Further, these results offer empirical evidence regarding the cognitive mediation process of experienced users in the post-adoptive context of household anti-malware software.

Fourth, our integrated moderated mediation analyses demonstrate support for Hypotheses 8 and 9 and explain *when* defensive avoidance users tend to process information in a biased way. Our results extend previous findings (e.g., [15, 50, 58]) by suggesting various contextual factors that may influence the security-conducive behavioral intention of experienced users. Specifically, we contextualize the moderation role of VUL proposed by the SMFAC (de Hoog et al., 2003) and the moderation role of UI (i.e., personal relevance) proposed by Gleicher and Petty (1992) and Liberman and Chaiken [55]. Consistent with the SMFAC, our findings indicate that high perceived VUL to the threat increases the mediation effect between DA and CONT. This finding suggests that VUL, which is strongly associated with PT, could be a moderating factor between DA and CONT. This finding also shows that DA does not always reduce adaptive responses (e.g., continued use of anti-malware software in an active way), but can facilitate them when users perceived high VUL. In addition, our study suggests that higher UI may enhance the biased cognitive appraisal process among defensive avoidance users. This study, therefore, extends existing findings based on classic fear appeal theories (e.g., [63], 1983), which assume that individuals tend to process fear-appeal messages in an objective and information-based way. Table 7

6.2. *Theoretical implications*

Most other IS security studies based on classic fear appeal theories have generally proposed that defensive motivation will result in security impairing behaviors or will undermine persuasion (e.g., [53]). This study provides another perspective by suggesting that defensively motivated individuals may process information in a security-conducive way if they perceive high vulnerability to the malware threat. This is in line with the SMFAC model's assumption that defensive motivation does not always undermine persuasion, but can sometimes facilitate it when individuals perceive themselves to be vulnerable to a highly relevant

Table 7
Summary of hypotheses

Hypothesis	Support?
H1: DA → PT (–)	Supported
H2: DA → PE (–)	Supported
H3: DA → CONT (–)	Supported
H4: PE → CONT (+)	Supported
H5: PT → CONT (+)	Supported
H6: PT → PE (+)	Supported
H7-a: PE mediate the relationship between DA and CONT (–)	Supported
H7-b: PT mediate the relationship between DA and CONT (–)	Supported
H7-c: PE mediate the relationship between PT and CONT (+)	Supported
H8: VUL moderates the mediation relationships between DA and CONT via PE	Supported
H9: UI moderates the mediation relationships between DA and CONT via PE	Supported

threat [18–20].

Second, analyses of the cognitive mediation process among defensive-motivated users revealed more insights into *how* information processing initiated by defensive avoidance affected behavioral intention; previous studies focused on the objective and information-based cognitive mediation process (e.g., [41, 72]). The study results suggested that when processing the security notification, individuals who perceived high vulnerability may experience more negative affect. To mitigate feelings of discomfort, they are motivated to minimize thoughts about the severity of threats. Their subsequent processing of the action recommendation, however, resulted in more positive thoughts about their perception of the efficacy of the recommendation. These positive thoughts of efficacy, together with minimized thoughts of the severity of the threat, mediated the defensive avoidance inclination on the subsequent behavioral intention.

Third, this study offers empirical evidence of how perceived vulnerability moderates the biased cognitive appraisal processing elicited by defensive motivation in response to security notifications. In comparison to users who perceived lower vulnerability, defensive-motivated users who perceived higher vulnerability towards malware threats tended to have a more positive expectation towards the effectiveness of the action recommendation but also tended to underestimate the severity of the malware threats depicted in the security notifications. The study results indicate that biased information processing about the security notification contributed to continued intention to actively use anti-malware software. These findings are in line with theoretical reasoning by Wiebe and Korbel [73], who propose that biased interpretation of threat information may not obstruct adaptive behavior but can facilitate problem-focused responses by suppressing potentially disruptive emotions.

Fourth, the present study shows how the role of user involvement can help to moderate cognitive appraisals under defensive motivation. Our study results suggest that user involvement could heighten biased information processing under defensive motivation. Specifically, this study revealed a positive bias in the processing of the action recommendation when users with high use involvement (e.g., users who perceived the potential consequences of malware threats to be highly relevant) expressed more positive thoughts about the recommendation than did users with low user involvement (e. g., users who perceived malware threats to have lower relevance). Although biased cognitive appraisal processing has long been hypothesized as a possible outcome of personal relevance (i.e., high user involvement) in psychology studies (e.g., [13]), this is the first study to probe the information processing and behavioral intention triggered by defensive avoidance in the context of household anti-malware software use by experienced users.

6.3. Practical implications

First, this study has important implications for understanding how users with defensive motivation process information. In previous studies, researchers have referred to the cognitive appraisal process as an objective and information-based calculation of the gain and cost associated with threat mitigation. This study suggests that, in addition to problem-focused coping, users may engage in emotional-focused coping, which is primarily aimed at reducing and controlling negative emotions through cognitive and behavioral regulation strategies. Our findings suggest to practitioners that defensive responses among home users of anti-malware software may lead to security-compromising behavioral intentions and, in the long run, may obstruct anti-malware software's effective protection of home computers.

Second, this study demonstrates how vulnerability perception influences information processing among defensively motivated users. Specifically, this study expands on previous findings by exploring the processing of the fear-eliciting messages (i.e., security notifications) and their impact on the intention to follow subsequent action recommendations. It provides more insights into the underlying processes that lead to security-inducing behavioral intention. Our results show that, instead of purely objective information processing, the cognitive appraisals and behavioral intentions influenced by defensive motivation are dominated by the level of perceived vulnerability. Thus, in the design of future security notifications, practitioners should consider communicating the vulnerability of home users when they are exposed to certain malware threats. We recommend that practitioners should highlight information about the vulnerability of home users to certain malware threats in order to prompt more security-conducive behavioral intentions.

Third, this study sheds light on the underlying processes related to how user involvement influences information processing and users' intentions to actively use anti-malware software on their home computers. One clear finding that has emerged from our study is the importance of user involvement in the enhancement of biased information processing and security-conducive behavior among defensively motivated users. Consider that a home computer can be accessed by multiple family members, each of whom may perceive varying levels of user involvement regarding the necessity to actively use anti-malware software. Thus, practitioners should consider stressing the psychological significance and highlighting the relevance of potential negative consequences of malware threats to various family members, which may encourage home users to engage in active use of anti-malware software on their home computers.

6.4. Limitations and future research

This study has some inevitable limitations. One limitation is related to the generalizability of the results. This research utilized an online survey of home users in the United States; therefore, some cultural differences may have impeded the explanatory power of this study for other populations [16]. All participants were employed at the time the research was conducted, and the sample included individuals with years of computer experience. As a result, the findings may have different explanatory power for different populations. Another limitation of this study is that the effect is not generalizable to other contexts. This study's focus on home computers may impede the explanatory effect in other contexts (e.g., workplace computing devices). Therefore, we suggest that future research studies further explore the potential contextual effects of the aforementioned factors.

Conclusion

While an unbiased or accuracy-motivated individual assesses personal relevant information in an information-based manner, the processing goal of defense-motivated individuals is to defend their preferred prior position and process information in a biased way. Our findings demonstrate that defensive-motivated home users tend to minimize security notifications, which may help them conserve cognitive resources and eliminate emotional distress. However, high perceived vulnerability and high user involvement may facilitate biased information processing, which may facilitate security-conducive behaviors. Our study provides a basis for integrating the moderation role of perceived vulnerability and user involvement into the information-processing perspective of fear-eliciting persuasion in household anti-malware software use among experienced users.

CRediT authorship contribution statement

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

Appendix 1. Constructs and measurement items

Perceived Threat [41]

THREAT 1 *Based on my past usage experience and general belief, I think* malware is a threat to my computer.
THREAT 2 *Based on my past usage experience and general belief, I think* the trouble caused by anti-malware threatens me.
THREAT 3 *Based on my past usage experience and general belief, I think* malware is a potential danger to my computer.

Perceived Efficacy [41]

EFFICACY 1 *Based on my past usage experience and general belief, I think* anti-malware applications work for computer protection.
EFFICACY 2 *Based on my past usage experience and general belief, I think* anti-malware applications are effective for computer protection.
EFFICACY 3 *Based on my past usage experience and general belief, I think* when using an anti-malware application, a computer is more likely to be protected from malware.

Perceived Vulnerability [41]

VUL 1 *Based on my past usage experience and general belief, I think* my computer is at risk of getting malware.
VUL 2 *Based on my past usage experience and general belief, I think* it is likely that my computer will become infected with malware.
VUL 3 *Based on my past usage experience and general belief, I think* it is possible that my computer will become infected with malware.

Defensive Avoidance [75]

DEFAVOID 1 *Whenever I am reminded about the need to use anti-malware software to prevent malicious software and to secure my home computer(s)*, my first instinct is to not think about the notification.
DEFAVOID 2 *Whenever I am reminded about the need to use anti-malware software to detect malicious software and to secure my home computer(s)*, my first instinct is to not do anything.
DEFAVOID 3 *Whenever I am reminded about the need to use anti-malware software to remove malicious software and to secure my home computer(s)*, I avoid thinking about the notification.

User Involvement [31]

USERINV1 *Indicate your thoughts concerning using anti-malware software in your home computer(s). I consider actively using anti-malware software in my home computer(s)* to be something that matters to me/doesn't matter to me.
USERINV2 *Indicate your thoughts concerning using anti-malware software in your home computer(s). I consider actively using anti-malware software in my home computer(s)* to be irrelevant to me/relevant to me.
USERINV3 *Indicate your thoughts concerning using anti-malware software in your home computer(s). I consider actively using anti-malware software in my home computer(s)* to be of no concern to me/of concern to me.

Continued Use Intention [41]

CONT 1 *Based on your past usage experience, to what extent will you continue using anti-malware software on your home computer*? I intend to prevent malicious software by actively using my anti-malware application on my home computer(s) in the next two weeks.
CONT 2 *Based on your past usage experience, to what extent will you continue using anti-malware software on your home computer*? I am likely to detect malicious software by actively using my anti-malware application on my home computer(s) in the next two weeks.
CONT 3 *Based on your past usage experience, to what extent will you continue using anti-malware software on your home computer*? I plan to avoid malicious software by actively using my anti-malware application on my home computer(s) in the next two weeks.

Items to check the poor-quality responses

For this question only answer 3, somewhat disagree; do not give any other answer.

For this question only answer 6, agree; do not give any other answer.

For this question only answer 2, agree; do not give any other answer.

References

[1] Accenture. (2021). 2021 cyber threat intelligence report. Retrieved September 6, 2021, from https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf.

[3] J.L Arbuckle, Amos 22.0 User's Guide, IBM SPSS, Chicago, 2013.

[4] H Barki, J Hartwick, Rethinking the concept of user involvement, MIS Q 13 (1) (1989) 53–63.

[7] S.J Blumberg, Guarding against threatening HIV prevention messages: an information-processing model, Health Educ. Behav 27 (6) (2000) 780–795, https://doi.org/10.1177/109019810002700611.

[8] B Bowins, Psychological defense mechanisms: a new perspective, Am. J. Psychoanal 64 (1) (2004) 1–26, https://doi.org/10.1023/B:TAJP.0000017989.72521.26.

[9] S.L Brown, M Richardson, The effect of distressing imagery on attention to and persuasiveness of an anti-alcohol message: a gaze-tracking approach, Health Educ. Behav 39 (1) (2012) 8–17, https://doi.org/10.1177/1090198111404411.

[10] S.L Brown, E.Z Smith, The inhibitory effect of a distressing anti-smoking message on risk perceptions in smokers, Psychol. Health 22 (3) (2007) 255–268, https://doi.org/10.1080/14768320600843127.

[11] S Brown, E Locker, Defensive responses to an emotive anti-alcohol message, Psychol. Health 24 (5) (2009) 517–528, https://doi.org/10.1080/08870440801911130.

[12] A.J Burns, T.L Roberts, C Posey, P.B Lowry, The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking, Inf. Syst. Res 30 (4) (2019) 1228–1247.

[13] S Chaiken, A Ledgerwood, A theory of heuristic and systematic information processing. Handbook of Theories of Social Psychology: Volume One, 2011, p. 246-166.

[14] S Chaiken, A Liberman, A.H Eagly, Heuristic and systematic information processing within and beyond the persuasion context, in: J.S Uleman, J.A Bargh (Eds.), Unintended thought, Guilford Press, New York, 1989, pp. 212–252.

[15] Y Chen, D.F Galletta, P.B Lowry, X Luo, G.D Moody, R Willison, Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model, Inf. Syst. Res (2021).

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

[18] E.H.H.J Das, J.B.F de Wit, W Stroebe, Fear appeals motivate acceptance of action recommendations: evidence for a positive bias in the processing of persuasive messages, Pers. Soc. Psychol. Bull 29 (5) (2003) 650–664, https://doi.org/10.1177/0146167203029005009.

[19] N de Hoog, W Stroebe, J.B.F de Wit, The impact of fear appeals on processing and acceptance of action recommendations, Pers. Soc. Psychol. Bull 31 (1) (2005) 24–33, https://doi.org/10.1177/0146167204271321.

[20] N de Hoog, W Stroebe, J.B.F de Wit, The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: a meta-analysis, Rev. Gen. Psychol 11 (3) (2007) 258–285, https://doi.org/10.1037/1089-2680.11.3.258.

[22] de Wit, J. B., Das, E., & de Hoog, N. (2007). Self-regulation of health communications: a motivated processing approach to risk perception and persuasion. In: The Scope of Social Psychology (pp. 221-238). Psychology Press.

[25] L Festinger, A Theory of Cognitive Dissonance (Vol. 2), Stanford university press, 1957.

[26] M.S Fritz, D.P Mackinnon, Required sample size to detect the mediated effect, Psychol. Sci 18 (3) (2007) 233–239.

[27] Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. MIS Q., III-XIV.

[29] C.H Hansen, R.D Hansen, D.W Shantz, Repression at encoding: Discrete appraisals of emotional stimuli, J. Pers. Soc. Psychol 63 (6) (1992) 1026–1035.

[31] J Hartwick, H Barki, Explaining the role of user participation in information system use, Manag. Sci 40 (4) (1994) 440–465, https://doi.org/10.1287/mnsc.40.4.440.

[32] A.F Hayes, An index and test of linear moderated mediation, Multivar. Behav. Res 50 (2015) 1–22, https://doi.org/10.1080/00273171.2014.962683.

[33] A.F Hayes, Partial, conditional, and moderated mediation: quantification, inference, and interpretation, Commun. Monogr 85 (1) (2018) 4–40.

[34] J Henseler, C.M Ringle, M Sarstedt, A new criterion for assessing discriminant validity in variance-based structural equation modeling, J. Acad. Market. Sci 43 (1) (2015) 115–135.

[35] C.M Jackson, S Chow, R Leitch, Toward an understanding of the behavioral intention to use an information system, Decis. Sci 28 (2) (1997) 357–389.

[36] D.L Jackson, Revisiting sample size and number of parameter estimates: some support for the N:q hypothesis, Struct. Eq. Model.: Multidiscip. J 10 (1) (2003) 128–141.

[41] Johnston & Warkentin, Fear appeals and information security behaviors: an empirical study, MIS Q 34 (3) (2010) 549, https://doi.org/10.2307/25750691.

[42] A.C Johnston, M Warkentin, M Siponen, An enhanced fear appeal rhetorical framework, MIS Q 39 (1) (2015) 113–134.

[43] P.A Keller, L.G Block, Increasing the persuasiveness of fear appeals: the effect of arousal and elaboration, J. Consum. Res 22 (4) (1996) 448, https://doi.org/10.1086/209461.

[44] L.T.E Kessels, R.A.C Ruiter, B.M Jansma, Increased attention but more efficient disengagement: neuroscientific evidence for defensive processing of threatening health information, Health Psychol 29 (4) (2010) 346–354, https://doi.org/10.1037/a0019372.

[45] L.T.E Kessels, R.A.C Ruiter, L Wouters, B.M Jansma, Neuroscientific evidence for defensive avoidance of fear appeals, Int. J. Psychol 49 (2) (2014) 80–88, https://doi.org/10.1002/ijop.12036.

[46] R.B Kline, Principles and Practice of Structural Equation Modeling, Guilford publications, 2015.

[47] Z Kunda, The case for motivated reasoning, Psychol. Bull 108 (3) (1990) 480.

[48] R.J Larsen, Toward a science of mood regulation, Psychol. Inq 11 (3) (2000) 129–141.

[49] R.S Lazarus, S Folkman, Stress, Appraisal, and Coping, Springer publishing company, 1984.

[50] H Li, X.R Luo, Y Chen, Understanding information security policy violation from a situational action perspective, J. Assoc. Inf. Syst 22 (3) (2021) 5.

[51] Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS Q., 71-90.

[52] H Liang, Y.L Xue, Understanding security behaviors in personal computer usage: a threat avoidance perspective, J. Assoc. Inf. Syst 11 (7) (2010) 1.

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

[55] A Liberman, S Chaiken, Defensive processing of personally relevant health messages, Pers. Soc. Psychol. Bull 18 (6) (1992) 669–679, https://doi.org/10.1177/0146167292186002.

[58] X.R Luo, H Li, Q Hu, H Xu, Why individual employees commit malicious computer abuse: a routine activity theory perspective, J. Assoc. Inf. Syst 21 (6) (2020) 5.

[60] M Mendolia, Repressors' appraisals of emotional stimuli in threatening and nonthreatening positive emotional contexts, J. Res. Personal 33 (1) (1999) 1–26, https://doi.org/10.1006/jrpe.1998.2235.

[61] D Muller, C Judd, Y Vincent, When moderation is mediated and mediation is moderated, J. Pers. Soc. Psychol 89 (6) (2005) 852–863.

[62] NTT. (2021). 2021 global threat intelligence report. Retrieved September 6, 2021, from https://www.key4biz.it/wp-content/uploads/2021/05/2021-Global-Threat-Intelligence-Report-full-report.pdf.

[63] R.W Rogers, W Deckner, Effects of fear appeals and physiological arousal upon emotion, attitudes, and cigarette smoking, J. Pers. Soc. Psychol 32 (1975) 222–230.

[64] R.W Rogers, Attitude change and information integration in fear appeals, Psychol. Rep 56 (1) (1985) 179–182.

[65] R.A.C Ruiter, C Abraham, G Kok, Scary warnings and rational precautions: A review of the psychology of fear appeals, Psychol. Health 16 (6) (2001) 613–630, https://doi.org/10.1080/08870440108405863.

[68] K.J Preacher, D.D Rucker, A.F Hayes, Addressing moderated mediation hypotheses: theory, methods, and prescriptions, Multivar. Behav. Res 42 (1) (2007) 185–227.

[69] Preacher, K. J., & Coffman, D. L. (2006, May). Computing power and minimum sample size for RMSEA [Computer software]. Available from http://quantpsy.org/.

[70] P.M Podsakoff, S.B MacKenzie, N.P Podsakoff, Sources of method bias in social science research and recommendations on how to control it, Annu. Rev. Psychol 63 (2012) 539–569.

[71] J van 't Riet, R.A.C Ruiter, Defensive reactions to health-promoting information: an overview and implications for future research, Health Psychol. Rev 7 (sup1) (2013) S104–S136, https://doi.org/10.1080/17437199.2011.606782.

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

[73] Wiebe, D. J., & Korbel, C. (2003). Defensive denial, affect, and the self-regulation of health threats. In L. D. Cameron & H. Leventhal (Eds.), The self-regulation of health and illness behaviour (pp. 184–203). Routledge.

[74] K Witte, Putting the fear back into fear appeals: The extended parallel process model, Commun. Monogr 59 (4) (1992) 329–349.

[75] K Witte, Fear control and danger control: a test of the extended parallel process model (EPPM), Commun. Monogr 61 (2) (1994) 113–134.

[76] K Witte, M Allen, A meta-analysis of fear appeals: implications for effective public health campaigns, Health Educ. Behav 27 (5) (2000) 591–615, https://doi.org/10.1177/109019810002700506.

[77] D.R Williams, M Sternthal, Understanding racial-ethnic disparities in health: sociological contributions, J. Health Soc. Behav 51 (1_suppl) (2010) S15–S27.

Yitian Xie is a PhD student in the Department of Information Technology at the University of Jyväskylä, Finland. She received her master's degree in psychology from East China Normal University, China. Her research interests center around individual information security behavior, security nudging design, information security education and training, and business strategy and analytics.

Mikko Siponen is a full professor of Information Systems. He has served as vice head of department, head of the department, and director of a research center. His degrees include Doctor of Social Sciences, majoring in Philosophy; MSc in Software Engineering; Lic. Phil. in Information Processing Sciences; and PhD in Information Systems. He has received over 10 million EUR of research funding from corporations and numerous other funding bodies. In addition to leading industry-funded projects, Mikko has been a PI on projects for the Academy of Finland, the EU, and the Finnish Funding Agency for Innovation. He has published more than 70 journal articles.

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

Xiaosong Zheng is a professor of Business Administration at Shanghai University, China. He received a PhD in IT from University of Oulu in Finland and a second PhD in Business Administration from Tallinn University of Technology in Estonia. He is also affiliated with University of Technology Sydney in Australia. He holds several master's degrees, including MSc in Accounting from University of Oulu, MSc in Economics from Hanken School of Economics, MSc in Computer Science from University of Tampere, and MEng in Robotics and Automation from Swinburne University of Technology. He has published widely in both business and IT fields.

III

DECLARATIVE AND PROCEDURAL INFORMATION SECURITY KNOWLEDGE OF THE GENERAL PUBLIC: CONCEPTUALIZATION AND INSTRUMENT DEVELOPMENT

by

Yitian Xie, Mikko Siponen (2022)

Unpublished Manuscript

Request a copy from author.