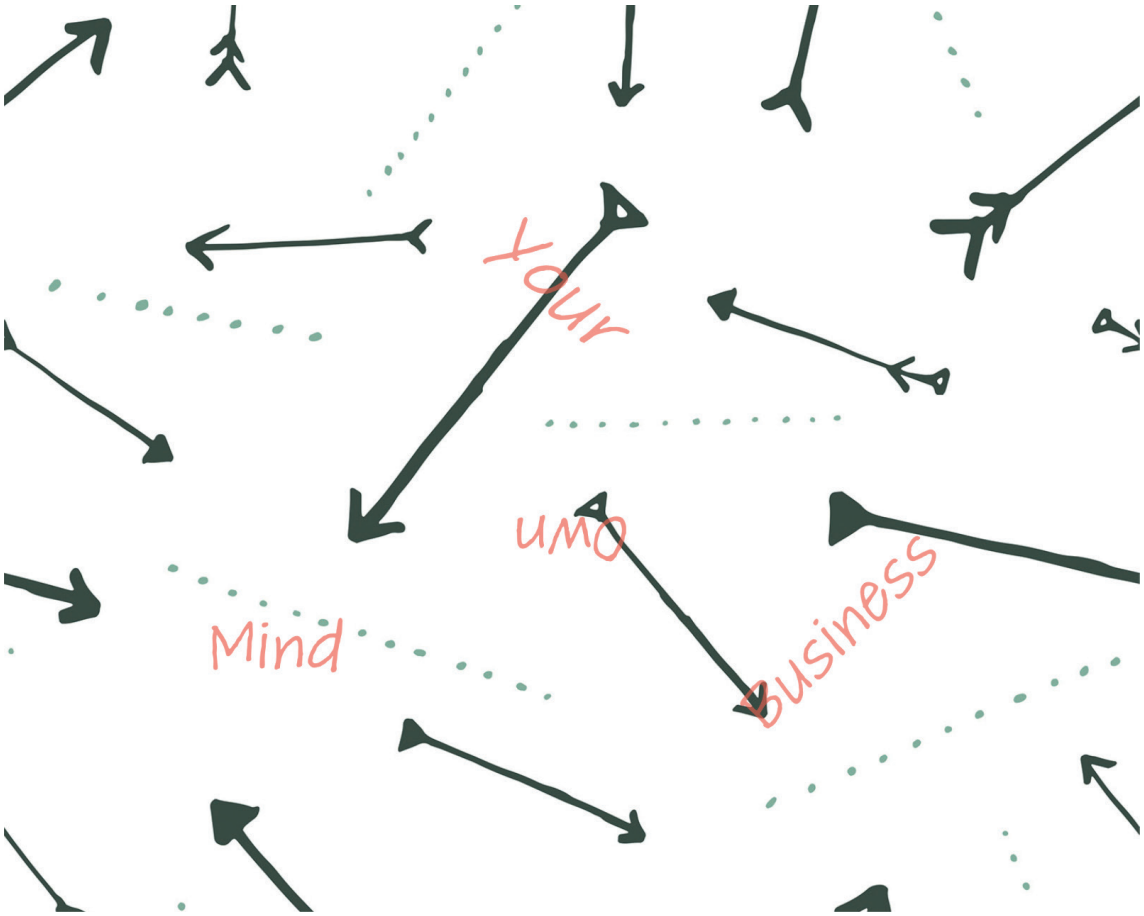
JYU DISSERTATIONS 504

Fufan Liu

Irrational Human Factors in Behavioral Information Security

Familiarity, Fear, and a Change of Mind



UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 504

Fufan Liu

Irrational Human Factors in Behavioral Information Security

Familiarity, Fear, and a Change of Mind

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 3
maaliskuun 28. päivänä 2022 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 3, on March 28, 2022 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2022

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

Cover picture by Fufan Liu.

ISBN 978-951-39-9090-9 (PDF)
URN:ISBN:978-951-39-9090-9
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-9090-9

ABSTRACT

Liu, Fufan
Irrational Human Factors in Behavioral Information Security: Familiarity, Fear, and a Change of Mind
Jyväskylä: University of Jyväskylä, 2022, 97 p.
(JYU Dissertations
ISSN 2489-9003; 504)
ISBN 978-951-39-9090-9 (PDF)

Behavioral information security (ISec) is an important research stream for management information systems (MIS) that relies on developments in other human sciences. In this dissertation, we investigate the psychological side of MIS by discussing the relationship between a few selected irrational human factors and persuasive information security communication.

In Study 1, we explore the role of familiarity on the perception of a range of information security threats and protective behavior. This topic is important and relevant, in that any type of ISec communication can get people familiarized with the broader topic of security and threat despite of its designed intention. The results show that familiarity could yield both positive and negative effects depending on how it is operationalized in the communicative setting. Study 2 was motivated by MIS's recent emphasis of "fear as the drive" in information security compliance, as well as the use of neuroimaging techniques to validate such fear. Along the chapter, we question the scientific understanding of fear and its measurement in behavioral ISec studies, and further argue that the inherent meaning of one general mental construct may vary to such a degree that a standardized measurement should be discouraged in MIS. Finally, in Study 3, we problematize the simple human capacity of being able to "change their mind" after making an initial decision. Based on discourses in behavioral economics and philosophy, a framework is proposed for portraying how one's able to have a change of mind, while the relationship between behavioral predictability and the individual's flexible use of information for decision support is emphasized. This framework explains why persuaded decision-making results may not last and how communication issuers may adapt a relaxed yet reflective implementation strategy to achieve more stable result in a longer lifecycle.

This dissertation contributes to MIS and ISec communication by exploring the foundational roles of three subtle yet crucial human factors, namely, familiarity, fear, and a change of mind. The discussions and results are linked to more generalized problems in MIS's pursuit of scientific and methodological rigor. Meanwhile, they imply great potential in embracing MIS's research possibilities in a human-centered direction.

Keywords: irrationality, behavioral information security, decision-making

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Liu, Fufan
Irrationaaliset inhimilliset tekijät tietoturvallisessa käyttäytymisessä: Tuttuus, pelko ja mielenmuutos
Jyväskylä: University of Jyväskylä, 2022, 97 p.
(JYU Dissertations
ISSN 2489-9003; 504)
ISBN 978-951-39-9090-9 (PDF)

Tietoturvallinen (ISec) käyttäytyminen on tärkeä johdon tietojärjestelmien (MIS) tutkimusalue, joka tukeutuu muiden humanististen tieteiden kuten psykologian kehitykseen. Tässä tutkielmassa tarkastellaan MIS:n psykologista puolta käsittelemällä muutamia irrationaalisia inhimillisiä tekijöitä ja niiden suhdetta suostuttelevaan tietoturvalliseen viestintään.

Tutkimuksessa 1 käsitellään tuttuuden roolia tietoturvallisuusriskien havaitsemisessa ja suojakäyttäytymisessä. Aihe on olennaisen tärkeä, sillä mikä tahansa tietoturvallisuusviestintä voi tutustuttaa ihmisiä laajemmin turvallisuuteen ja turvallisuusriskeihin. Tutkimustulokset osoittavat, että tuttuus saattaa tuottaa sekä positiivisia että negatiivisia vaikutuksia riippuen siitä, millä tavalla sitä kyseisessä viestintäympäristössä käytetään. Tutkimuksen 2 taustalla vaikutti MIS:n viimeaikainen painotus "pelosta ajavana voimana" tietoturvallisuuden noudattamisessa sekä neurokuvatekniikoiden käyttö tällaisen pelon vahvistamiseksi. Tietoturvallisen käyttäytymisen tutkimuksissa esiintyvä tieteellinen käsitys pelosta sekä sen mittaamistavoista kyseenalaistetaan. Edelleen argumentoidaan yksittäisen ajatusrakennelman luontaisen merkityksen voivan vaihdella kontekstista riippuen niin suuresti, ettei standardoituja mittaamistapoja voi suositella MIS:n tutkimuksiin. Tutkimuksessa 3 tarkastellaan kriittisesti ihmisten kykyä "muuttaa mieltä" jo tehdyn päätöksen jälkeen. Käyttäytymistalouden ja filosofian diskursseihin perustuen ehdotetaankin mielenmuutoksen kykyä kuvaavaa viitekehystä, jossa korostuu käyttäytymisen ennustettavuuden ja yksilön joustavan tiedonkäytön välinen suhde päätöksenteon tukena. Tämä viitekehys selittää, miksi suostuttelun vaikutuksesta tehdyt päätökset eivät välttämättä ole pysyviä, ja kuinka viestijät voisivat hyödyntää rennompaa mutta ajatuksia herättävää viestintästrategiaa saavuttaakseen pysyvämpiä tuloksia pidemmällä aikavälillä.

Tämä tutkielma edistää tietoturvallisuuden tutkimusalaa tutkimalla hienovaraisten mutta merkittävien inhimillisten tekijöiden (tuttuus, pelko ja mielenmuutos) perustavanlaatuisia rooleja. Aiheen käsittely ja tulokset liittyvät yleisiin ongelmiin MIS:n pyrkimyksessä tieteelliseen ja metodologiseen tarkkuuteen. Toisaalta ne viittaavat MIS:n huomattavaan potentiaaliin omaksua ainutlaatuisia ihmiskeskeisiä tutkimusmahdollisuuksia.

Avainsanat: irrationaalisuus, tietoturvallinen käyttäytyminen, päätöksenteko

Author Fufan Liu
Faculty of Information Technology
University of Jyväskylä
Finland
fufanliu@outlook.com
orcid.org/0000-0002-5430-0434

Supervisors Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers John D'Arcy
Department of Accounting and Management Information Systems
University of Delaware
USA

Huigang Liang
Department of Business Information and Technology
University of Memphis
USA

Opponent Paul van Schaik
Department of Psychology
Teesside University
UK

ACKNOWLEDGEMENTS

During no period of time was my doubt of the work-life continuity and the agony over unclarity felt more strongly than during my doctoral studies. As necessary as they are, and for the fruition they have come to bear beyond this dissertation, I would like to express my gratitude to people with whom I was lucky to be connected with in the actualization of my research work, and to those who stood by me and connected with me in different ways.

First and foremost, I am deeply grateful to my supervisor Prof. Mikko Siponen, whom I was incredibly lucky to have met, known, and worked with along my way of academic growth. It was him who sparked my genuine interest in the philosophy of science and the initial idea for my doctoral research. His comments and teaching were efficient and insightful, from which formed some of my most fundamental academic concerns. I appreciate his intellectual and critical feedbacks for my dissertation and the studies involved. More importantly, I feel honored to regard him as my role model in being a researcher and in the pursuit of the strengthening of the mind and the body.

Crucially, regarding the publication of the dissertation, I want to thank Prof. John D'Arcy and Prof. Huigang Liang for their review and kind comments on my work, based on which I was able to polish the dissertation and reflect on future research direction. I sincerely thank Prof. Paul van Schaik, for accepting to be my opponent and committing efforts to examining my work. Furthermore, I deeply thank Prof. Teresa Garcia-Marques, for her kind guidance and hospitality I would never forget.

I wish to give special thanks, both as a collogue and a friend, to Dr. Wael Soliman, Dr. Hojat Mohammadnazar, Tong Xin, Truth Lumor, and Yitian Xie, for the interesting academic discussions we had, shared faculty time, and some of the warm camaraderie outside of the university. Specifically, I would like to thank Prof. Steffi Haag and Dr. Xiuyan Shao for having me as a collaborator in research projects apart from the studies involved in this dissertation.

It would be in relation to the inspirations and struggles in the larger context of life, that one's work concerns and problematization becomes more significant. For this, I hold the greatest appreciation to Luna, with whom even the most mundane details in life could be sensed as glowing, sublime, and discussable in an entrancing fashion. It was through the loving dialogues, meditative pauses, and formidable challenges we leapt through, that I did not find, but was found by a state of flux which exceeds precise rationality. Beyond words can express, I am extremely grateful for the unbounded times we shared together.

The following acknowledgements, while not directly relevant to the work of this dissertation, are crucial for my personal and social growth as a sane and caring human being.

I feel obliged to thank three friends who are significant to me throughout the good and bad times in life. I give my very special gratitude to Alex, for his compassionate heart, dependable presence, energetic creativity, the eloquent collaboration we had, as well as our strong friendship tested against time. I am

profoundly grateful to Sofia, for the sincere conversations, her enormous support to my mental stability, and the indisputable discussions we had on faith and belief. I also thank her for the thorough and careful translation of the Finnish abstract in this dissertation. Moreover, I hold deep appreciation to Anne, for her exquisite wandering spirit, delicate emotional support during the pandemics, and those hearty vegan recipes we cooked.

Over the years, I have come across dependable friends, among whom some had left the temporary lodge of Jyväskylä, and others stayed. I am grateful to Zihan and Xiaoguang, for the irreplaceable times we had together and the fellowship we came to form. I am very thankful to my previous neighbor Timo and Saara, for their hospitality and long-term support as friends. I deeply appreciate Jennifer, Svetlana, Minjee, Jesse, and Anduena, for simply being there wonderfully at the beginning of my stay in Finland. I am grateful to Hao, Yixue, and Jian for their supportive company with trustworthy notes and tips. I hold much appreciation for Eureka's generous supply and kind help. I am happy to thank Yogesh, Kris, Heidy, and Johanna, for their supports and the photographs we made in the summer. I really appreciate Dr. Yan Liu, for her remarkable treats, lifestyle support, and festive moods in every gathering. I am thankful to Xueqiao and Dr. Qianru Xu, for the occasional but inspiring notes we share. Moreover, I would like to thank Francesca for her psychological support and the amazing food, thank Vivian for our spiritual connection in the distance, and thank Qingyang & Brie for their heartful host in Oulu painted with chilled vibes. I want to thank Chaoxiong, particularly, for the life tips and the grim yet cheerful conversations we had. I wish to thank Maryam, considerably, for her confidence and enthusiasm in arts & science, and the co-exhibition we hosted together with Alex. Still, my heartfelt appreciation goes to Shawn and Nyx, for our excellent time in Sweden, and for they beautifully showed me a different way of living, working, and feeling the Nordic.

Last but certainly not the least, the warmest and most loving appreciation goes to my parents, for their love transcending words, space, and difficulties through the years. I feel sorry for having missed those more-than-important turning points, but I believe positive forces have just set off and many happy moments will return.

I see a path of research and life projects formed, fair and square, branching from the closure of my doctoral research concerns, and beaming along the beginning of something more substantial.

Jyväskylä 2.3.2022
Fufan Liu

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

While the engineering of technological means to counteract information security (ISec) threats are necessary, human factors often plays an even more significant role (Metalidou et al., 2014) in security breaches, the cause of which relates to various insecure human actions, such as email misuse (e.g., phishing email), privilege misuse, social engineering, and password reuse, among others (*2021 Data Breach Investigations Report*, 2021). In management information systems (MIS) research, the study of ISec behaviors (Stanton et al., 2005) is an important field that directs the conception, design, and implementation of behavioral interventions in mitigating digital threats, which contributes to safer environments for the use of information systems (IS) in both public and private dimensions (Li & Siponen, 2011; Siponen, 2001).

The general discipline of information systems has drawn upon many other disciplines as itself being a young branch of social science (Baskerville, 2002; Keen, 1980), which is also the case for behavioral information security. Among the reviewed 11 most-used theories for explaining information security behaviors in Moody et al. (2018), six originated in psychology, three in criminology, and two in public health. For instance, perhaps the most studied risk avoidance theory in behavioral ISec, the protection motivation theory (PMT, Maddux & Rogers, 1983; Rogers, 1975, 1983; Rogers & Steven, 1997), was originally developed and applied in health psychology for many years (Floyd et al., 2000; e.g., Rogers & Mewborn, 1976; Rogers & Steven, 1997) before key ISec literatures borrowed it to explain IT-related risk and threat avoidance (e.g., Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010).

For the practical purpose of ISec management, different mental and behavioral interventions need to be designed and distributed to different contact levels with various modes of delivery, such as written ISec policies for employees in organization (Siponen et al., 2014) and computer security warning for individual home users (Vance et al., 2018). My doctoral research begun with reviewing the historical development of PMT in psychology and its primary applications in MIS on implementing and measuring the effectiveness of an important type of persuasive intervention known as *fear appeal* (Johnston &

Warkentin, 2010), which can be characterized as a set of fear-arousing stimuli (e.g., written statements and suggestions on ISec practice) that depict negative consequences of harmful behaviors while seeking to eliminating such behaviors by promoting recommended coping methods (Rhodes, 2017; Rogers, 1975; Witte, 1992). Historically, PMT was first developed in health psychology to explain how people systematically response to such fear appeal interventions (Maddux & Rogers, 1983; Rogers & Steven, 1997) by highlighting a set of factors that affect human's cognitive appraisal of health threats and coping methods to negate those threats.

I was initially involved in a research project that eventually produced a general review of PMT and its use in IS (Haag et al., 2021), as well as a critical analysis on the misunderstandings of PMT among IS scholars (currently under peer review). In parallel though, my research attention and reading interest was drawn to more abstract problems regarding how IS studies present theories and constructs from psychology, the theoretical nature of which is eventually connected to the pursuit of designing effective fear appeal implementation that is less likely to fade away or backfire in practice (Ruiter et al., 2014; Wall & Buche, 2017). While a number of prominent IS studies focused on identifying, integrating, implementing, and fine-tuning persuasive factors within and outside of PMT (e.g., Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010; Moody et al., 2018; Orazi et al., 2019; Wall & Warkentin, 2019), in order to empirically test variations in their persuasive results, I became more interested in revisiting subtler psychological constructs that IS scholars may have taken for granted across studies, the discussion of which forms the three main chapters of this dissertation. Specifically, the phenomenon I discuss can be summarized and termed in the following highlighted keywords in mundane sayings, such as "people's *familiarity* with what they see", "their *fear* towards undesirable threats", and "the common capacity that a human being is able to *change their mind*". While such mental factors are not the normal focus in information security management, I hold that these targeted discussions would positively affect fellow scholars' understanding of persuasive techniques/theory for MIS, as well as reflecting on the nature of scientific rigor in MIS. Next, I explain my motivation/inspiration in the initial contemplation of those topics.

In the discussion of potential solutions for improving fear appeal implementation, prospective IS studies suggested future research keep exploring and refining factors that would inform improved model structure and statistical fitness (Boss et al., 2015), or focusing on specific behavioral "pathways" within the entire model, such as identifying the appropriate amount of elicited fear for improved persuasive results (Wall & Buche, 2017). However, my research drive lies in a psychological track at the foundation of the sole pursuit of improved persuasion. First, any implementation of ISec communication and persuasion efforts, regardless of its intended effects, always familiarizes people of some general information of ISec threats. To study questions such as "if repeated ISec fear appeal campaigns are effective for achieving resistant results", one may benefit by first of all studying the effect of the basic perceived familiarity of ISec on persuasive results. If the effect of such fundamental factor varies with contexts,

it would be no wonder that "repeated campaign" per se does not ensure persistent results. Second, for fear appeal and its base theory to work expectedly, the meaning and implementation of constructs such as "fear" should ideally be consistent across studies and contexts. Otherwise, it would be not feasible to even compare different research results in the first place, let alone seeing such comparison as meaningful for theoretical improvement, such as if fear should be high or low enough to achieve certain level of persuasive effect. On a larger scale, if borrowed theories and constructs are understood and implemented differently but claimed or implied to be the same across different discursive arguments, the discussion of theoretical contribution may only proceed in the manipulation of a language play. The priority of IS studies, in my vision, is not knowledge and theory described in consistent linguistic terms, but the unique portraying of key constructs' actual operationalization in context. Finally, while reference theories for fear appeal offer frameworks to model human's rational risk avoidance behaviors, we should keep in mind that a human being is most likely to be capable of having a change of mind. Such obvious yet subtle phenomenon could be at the foundation of ISec communication's backfiring. Note that such capability of one's changing mind does not need to be discussed in relation to the human potential of free will, but simply due to the arguable fact that any person can make decisions by incorporating information in addition to received ISec communication at one time. Consequently, such simple consideration, as I show later, reflects a general framework which explains how human decision-making patterns change over time and context. Call for these considerations has been proposed in IS (Dennis & Minas, 2018) but few studies attempt to explore further.

As the response for any question could be approached conceptually or anchored with more specific arguments, the three main chapters of this dissertation address previous concerns in respective ways. In Chapter 2, an empirical study is carried out to study the effect of familiarity on common ISec threats. The result suggests that the familiarity of ISec threats could have both positive and negative effects depending on different communication conditions. In Chapter 3, I present a critical analysis on the understanding of fear in IS based on established empirical evidence and discourse in the psychology and philosophy of affective process. The results question some fundamental implications and understanding of the affective construct of fear in MIS, at the same time informing more research possibilities in the future. In Chapter 4, I portray the predictability of long-term persuasive outcomes of ISec communications with a framework that explains how human engage in the simple mental act of having a change of mind, the result of which not only provides implications for the flexible use of behavioral theory in IS behavioral interventions but argues for an ISec persuasive strategy that takes advantage of diversified information sources for informed and human-centered ISec decision-making.

While my initial research endeavor was to find a "know-how" solution for developing persuasive implementations that achieves effective ISec results, I have eventually chosen to discuss aforementioned topics regarding irrationalities in the research and practice of ISM, the discussions of which deconstruct a simple

and typical pursuit of a "know-how" for mitigating threats. Overall, I wish my discussion would produce echoes in the field and promote more human-centered persuasive design strategies.

2 STUDY 1: WHEN INCREASED INFORMATION SECURITY COMMUNICATION LEADS TO DECREASED PROTECTIVE BEHAVIOR

Citizens receive information with intended or unintended persuasive purposes such as information security (ISec) educational activities or just ISec-related news. It is often assumed in the ISec literature that increased familiarity with ISec threats tends to increase protective behavior (intention). However, following literatures in psychology, we argue that increased familiarity could increase risk perception for ISec threats, but only for simple stimuli people are less familiar with initially. In turn, the more may not be the better. Increased complexity of communicative material and increased familiarity with threats may result in decreased behavioral coping rate.

To examine this, we conducted an experimental study to explore the role of familiarity and communicative material's complexity (the level of implanted informativeness) in behavioral ISec persuasion. Specifically, we examined the impact of familiarity on risk perception for 32 common security risks. The findings support our hypotheses: Increased familiarity increased risk perception, but only for simpler communication stimuli that people were not familiar with to start. With more informative stimuli, increased familiarity even decreased ISec behavioral coping rate while maintaining a superficial level of risk perception. Our research raises an alarm for the effects of overexposed and negatively informative ISec contents. Overall, we offer three major contributions and two minor contributions.

2.1 Introduction to Study 1

A key research stream in information systems (IS) is understanding and improving users' information security (ISec) behavior. Typical ways to improve include interactive educational activities (e.g., Puhakainen & Siponen, 2010) or one-way campaigning messages, such as fear appeals (e.g., Boss et al., 2015;

Johnston et al., 2015). But citizens could also encounter ISec content with little intended persuasive purpose, such as ISec-related messages in news, films, TV series. All these sources may increase their familiarity with ISec threats, but it seems not certain familiarity always contributes to subsequent risk avoidance.

It is the contention of this study that increased familiarity could have a negative effect on ISec perception and behavior. Many ISec scholars have applied health threat theories from psychology to explain security intentions and behaviors (e.g., Boss et al., 2015, 2015; Johnston et al., 2015). But people at risk of a certain health threat are often more likely to reject the health-promoting messages more familiar to them (Liberman & Chaiken, 1992; Ruiter et al., 2014; van 't Riet & Ruiter, 2013). Studies on message exposure have found that overexposures can lead to negative effects (Montoya et al., 2017), and the effect of familiarity is related to people's initial aptitude for persuasive materials (McCoy et al., 2017). Furthermore, ISec communication often involves technical terms and relevant knowledge people may not be able to understand (Samsudin et al., 2016; Sunshine et al., 2009; Zaaba & Boon, 2015). Combining available evidence, we argue that increased familiarity could increase ISec risk perception, but only for simpler (i.e., less informative, in our setting here) stimuli with which people are not initially familiar with. In turn, more complicated and informative ISec communication may generate an illusion of knowing which results in decreased persuasive effects.

In our study, we are interested in how familiar with ISec threats, as a manipulatable independent variable, may contribute to persuasive outcomes. This topic may be especially relevant for people who hold limited understanding of ISec and who are potentially more subject to the effect of familiarity. Since the concept of familiarity has never been formally discussed in IS, we first review relevant literature and offer a definition. Then we discuss the potential role of familiarity in security communication as well as our research context. Next, we empirically test the influence of familiarity on ISec perception and behavior. Finally, we discuss the results and their implications. Overall, our study offers three major and two minor contributions to the ISec literature. We show that increased familiarity with ISec may lead to a superficial "knowing" while undermining persuasive outcomes such as protective behavior in practice.

2.2 On the Meaning of Familiarity

Research on familiarity dates to the 1960s (Greenwald & Sakumura, 1967; Higbee, 1969; Keller & Block, 1996; Thomas et al., 1961) when studies adapted subjective self-reporting for its measurement. Later, the notion of a subjective feeling of familiarity (Garcia-Marques & Mackie, 2001; Moons et al., 2009; Whittlesea & Williams, 2000) was proposed to indicate the subjective nature of familiarity as a vague feeling. However, some researchers (i.e., persuasive studies that adapt threat-related messages) also referred to "familiarity" in a "rational" sense. Rogers (1975, p. 104), for instance, regarded the familiarity with fear-based

appeal messages as a more-or-less correct appraisal. Similarly, Lucassen (2010) argued that Internet users evaluate the trustworthiness of familiar Wikipedia entries based more on correctness, addressing familiarity as an ability to correctly evaluate facts.

The two interpretations of familiarity have blurred the line in between a vague feeling of familiarity and an intellectual evaluation. As it is indeed hard to set the line beyond which one intentionally understands something instead of simply feeling it, we characterize familiarity as a subjective feeling *with or without* certain level of deliberate understanding in presence. It may be operationalized as subjective reporting, external criteria, or a mixed of both depending on the context and purpose of study. In other words, we acknowledge that this notion can mean differently across studies, while retaining the use of the same linguistic label of "familiarity".

Notably, while one may consider familiarity as a unidimensional continuum ranging from a pure feeling to full rational understanding, an individual may feel extremely familiar with something without actual understanding, especially in terms of its reflection in numeric measurements. For example, a layperson with no technical understanding could be highly interested in a new ISec threat, thus rating it as very familiar. However, a junior student could technically know more about this threat, yet at the same time gets puzzled by its engineering method, hence rating it as less familiar on paper. As previously found, self-perceived familiarity does not necessarily have to be in line with externally specified measures (Bacon, 1979), although one may be led to rate familiarity based on clear or calculatable standards.

To further clarify the meaning of familiarity, the concept of familiarity is compared to security fatigue (Cram et al., 2021; D'Arcy et al., 2014), where security related decision making, behavior, and emotional state can be negatively affected by over-implemented persuasive attempts. While security fatigue is characterized by the human agent's conscious realization (e.g., the individual explicitly feels tired or gets bored with long and bulky policy terms), the notion of familiarity, in our characterization, points to a state that can be emotion-independent and consciousness-independent. One can be fatigued by something while naturally obtaining ample familiarity, but one can also be familiar with something without any fatigue or eve consciously knowing. In our study, we are interested in the kind of familiarity citizens gain in more neural channels free from specific and intentional security campaigns, as further explained in Section 2.4.3.

2.3 Familiarity and Persuasion

In this section, we briefly review studies from psychology on the role of familiarity in persuasion (Section 2.3.1), which is necessary to understand its persuasive significance. Then we review how existing ISec works related to

familiarity (Section 2.3.2), albeit important, are not about "familiarity" in the sense that we use the term (Section 2.3.3).

2.3.1 Familiarity Research in Psychology

In nonthreatening communication, it was found that people tend to be more in favor of repeatedly exposed messages, which has been summarized as the "mere exposure effect" (Montoya et al., 2017; Silva, 2014). Consumer psychology has further suggested that more familiarity of advertisements leads to more likeness of products within an adequate exposure range (Campbell & Keller, 2003; Nepomuceno et al., 2014; Yao & Li, 2008). Cognitive psychology has also argued that higher message acceptability could be promoted by a simple feeling of familiarity (Garcia-Marques & Mackie, 2001; Moons et al., 2009), where repeatedly exposed stimuli tend to be preferred than novel stimuli (Montoya et al., 2017; Silva, 2014).

However, familiarity could also lead to negative persuasive results. The effect of familiarity could be related to people's *initial aptitude* for persuasive materials. Thus, with online advertisements disliked in the first place, repetitive presentation may result in increased perceived negativity (McCoy et al., 2017). Moreover, when ads are presented too frequently, a negative effect may also happen (Gillebaart et al., 2012; Reinhard et al., 2014). In health psychology research, which ISec often refers to (Moody et al., 2018), it was found those mostly at health risk are also more likely to reject the health risk communications they are often exposed to (Liberman & Chaiken, 1992; Ruiter et al., 2014; van 't Riet & Ruiter, 2013), sometimes accompanied with fundamental cognitive biases, such as attention disengagement (Kessels et al., 2010) and defensiveness (Kunda, 1987). A recent study in health psychology (Shi & Smith, 2016) showed that repeated exposure to health risk communication increased heuristic thoughts and perceived threat, but not self-efficacy or action intention. Familiarity, in this case, affected intermediate evaluative constructs, but not the final persuasive result.

2.3.2 Related Work in IS and ISec

While no study has dedicated to the concept of familiarity in ISec research, some studies did include what may be regarded or called as "familiarity", as one of the constructs in their correlational designs (Alraja et al., 2019; Amran et al., 2018; Huang et al., 2007, 2010; Jeske & van Schaik, 2017; Nepomuceno et al., 2014; van Schaik et al., 2017; Vance et al., 2018). A few studies implemented variables such as "media exposure" and "security awareness" with surveys (C. L. Anderson & Agarwal, 2010; Yang & Lee, 2016). However, general media exposure may not equal familiarity with a specific threat in a particular study. Huang (2010) included "familiarity" and "understanding" of ISec threats in a higher-order category named "knowledge". But in our characterization, familiarity can be independent from straightforward knowledge. Shillair et al. (2015) used self-reports to distinguish users with different knowledge levels on ISec threats, which is not the feeling-based familiarity (Garcia-Marques & Mackie, 2001) we

wish to implement in our study. In Sohrabi Safa et al. (2016), the concept of experience was used to incorporate the totality of knowledge, mastery, familiarity, ability, skill, etc., without directly addressing familiarity specifically. Furthermore, even when free of any report bias in these survey-based studies (Ruiter et al., 2014), probabilistic causal relationships cannot be inferred without empirical manipulations.

Among the ISec studies that measured constructs claimed as "familiarity" and yielded mixed results, no study has addressed our concern of familiarity with specific communication materials. Parsons (2010) proposed that familiar risks are likely to be underestimated, hence leading to less secure practice. However, one may also argue the opposite based on Ortiz et al. (2000), according to which people conform more to ISec practice while using products with which they are more familiar with. A more recent survey (Jeske & van Schaik, 2017) found that people who are more familiar with ISec threats are more likely to commit to ISec behaviors. In other contexts, familiarity may undermine risk perception in indirect ways. For example, Alraja et al. (2019) found that familiarity increased trust in using IoT-based healthcare, which then reduced perceived risk for practical usage. Empirical studies (Amran et al., 2018; Bravo-Lillo, 2014; Vance et al., 2018) on computer security warnings, though, have proposed a "habituation effect" in which more repetitions of the same warning window quickly led to cognitive exhaustion or ignorance. Besides positive and negative persuasive outcomes in opposite directions, Mäenpää (Mäenpää et al., 2008) found that ISec was not a concern for users in using online banks, regardless of their familiarity with the online banking system.

As reviewed, previous psychological studies have not used IT-related threatening materials to study the effect of familiarity. ISec studies, on the other hand, have not defined or studied familiarity with experimental controls. With mixed results and familiarity's potential significance in the current media-enriched human digital lifestyle, it is highly valuable to study its causal role for persuasive results for in behavioral ISec.

2.3.3 Contextualizing Familiarity

Familiarity may build up whenever human engage in attention switch and maintenance for a range of different stimuli (Cranor, 2008). With what Postman (1987, 2006) summed as "media as epistemology", the familiarity encapsulated in different channels and forms may embed varied qualities. For example, a comedy script may highlight ISec threats, but the hilarious tone of the medium could render the familiarity qualitatively different from the familiarity one gains in a seriously toned documentary. Thus, one is not likely to observe a fixed effect of "familiarity" as if it is a standalone physical entity by its own.

Specifically, we are interested in two general contexts in practice: the familiarity one obtains from a simple non-informative stimulus and the familiarity one obtains from more complicated (i.e., informative) communicative forms that involves assumed knowledge promotion. A typical scenario in which people could become more familiar with ISec may be the accumulation of

repetitive exposures to simple, non-informative security terms or names. For example, it is easy to imagine a pedestrian passing a street poster about security risk, but only paying minimal attention to the title (name-only). A sense of superficial familiarity may stay in vacancy of any information that contributes to comprehension and knowledge expansion. This may be more prominent for people who already have a relatively low level of understanding of ISec issues to begin with, or some elderly who barely know how computers work and only pay attention to IT-related information in the simplest form. Alternatively, one may be exposed to ISec communications which do promote concrete knowledge, and which do require conscious processing. Previous research in ISec suggested that users often do not understand security warnings (Samsudin et al., 2016; Sunshine et al., 2009; Zaaba & Boon, 2015) because of the technical jargon used, users' incorrect mental models, and a lack of experience, even though security warnings in commercial software may be designed based on established user interface design guidelines. In this case, we are especially interested in how familiar people are *already* with common ISec threats presented in a knowledge format and how the repetitive exposure of such information affects risk perception.

To reduce bias for a particular type of medium, we intend to implement a basic, yet still representable context, in which the most concise forms of ISec communication are implemented. In the following section, we implement an experiment to study the effect of familiarity on persuasive outcome (i.e., risk perception and protective behavior) adapting a known experimental method from social-cognitive psychology (Garcia-Marques, 2000; Garcia-Marques & Mackie, 2001; Moons et al., 2009). While such a method is not previously used in ISec to our knowledge, it has been commonly used to study familiarity's effect on persuasion in psychology. Our tailored design allows us to approximate the role of familiarity for ISec threats with precise experimental controls, but without high-cost social experiments that could also involve more confounding variables.

2.4 Behavioral Experiment: Familiarity and ISec Risk Avoidance

In our experiment, we explore the effect of repetitive exposures on security perception for 32 common ISec threats under two communication complexity levels (simple vs. informative). We intent to highlight two basic endeavors to increase familiarity. For one, communicative material can be repetitively presented, which we refer to as repetition-based familiarity (e.g., one runs through the same ISec news title over time). For the other, communication issuer could enrich the material's complexity in hope of inciting more familiarity with understanding (e.g., the user scrolls through the entire privacy agreement before being able to press the "agree" button). We form the following basic hypothesis based on previous discussions, with regard to our research design and scenario:

H1. Repetition-based familiarity increases risk perception of ISec threats, but more so with simple communication materials (supported).

H2. Repetition-based familiarity increases risk perception of ISec threats, but more so for threats the participants are less familiar with to start (supported).
H3. More communicative complexity or informativeness could negatively affect the risk avoidance behavior (supported).
H4. Repetition-based familiarity has more effect on persuasive results when the communication material is simpler (supported).

Other findings are also discussed later in the study.

2.4.1 Participants

A Chinese university contributed 102 students (65 females and 37 males) to the study. The average age of the participants was 26.28 (SD = 4.44). They majored in a variety of backgrounds, with 12 in business, seven in computer science, eight in engineering, seven in finance, 28 in liberal arts, five in medical science, three in natural science, 22 in social science, one in math, and nice in other minor subjects. 17 participants have had some kind of training in information technology, but no one majored or was specialized in information security or cybersecurity. As we utilize a psychological experiment in which participants rate three metrics (i.e., perceived familiarity, understanding, and risk) multiple times across *multiple trials*, the behavioral errors (e.g., random errors in reaction time) should stabilize over trials (Bellemare et al., 2014; Kerlinger, 1986) and the number of participants needed should also be much less than what is typically needed in an IS survey study with numerous variables and regression models. Also, the sample size here is comparable to previous studies which used the same experimental method for the study of familiarity (Garcia-Marques, 2000; Garcia-Marques & Mackie, 2001; Moons et al., 2009).

2.4.2 Design and Procedure

We manipulated the increase of familiarity with a behavioral experiment that makes use of repetitively presented information, which has been used in previous research, such as Garcia-Marques (Garcia-Marques, 2000), Garcia-Marques and Mackie (2001), and Moon et al. (2009). In this method, we operationalized familiarity as different times of repetitive exposure (one vs. two times), and ISec threats as written texts of "only names" (simple condition) or "names coupled with explanatory information" (informative condition). The procedure is as followed.

All participants completed the experiment task with a computer. The experiment program was made with Lab.js (Henninger et al., 2019), which runs on most modern web browsers. As illustrated in Figure. 1, it was composed of an introductory block followed by 4 main tasks. During the introduction, participants signed the experiment consent, then proceeded to the instructions and three trials followed as practice, which were formally identical to those in the main tasks. They were randomly assigned into either *the simple condition*

(threats presented as title only, N = 51) or *the informative condition* (threats presented with informative explanations, N = 50). Next, they proceeded to task one, in which ISec threats were randomly presented in each rating trial. Randomization is a standard practice in psychological experiment design (Hacking, 1988) to reduce potential order effects (e.g., the evaluations of risks at the start may be rated differently) and fatigue (Grant, 1948). Within each trial, a fixation cross was first displayed for 500ms (Zokaei et al., 2014) to attract a participant's visual attention to the center of a screen. Then the program showed a security-related title briefly (700 ms), followed by three questions displayed below the title of ISec threat one by one, where participants rated their perceived familiarity (response time limited to 15s to avoid excessive deliberate thinking), perceived understanding (no time limit) and perceived personal risk (no time limit). Ratings of familiarity always appeared first to avoid potential influence from the other two ratings if they were presented first. The order of ratings for understanding and severity was randomized so their potential influence on each other may be counterbalanced. Notice that at this point, the experiment program not only manipulated the presentation of threat stimuli along with the questions, as well as measured the baseline familiarity and understanding participants have towards the threats. In other words, the manipulation of exposing something one time would be equivalent to a baseline measurement of their initial familiarity.

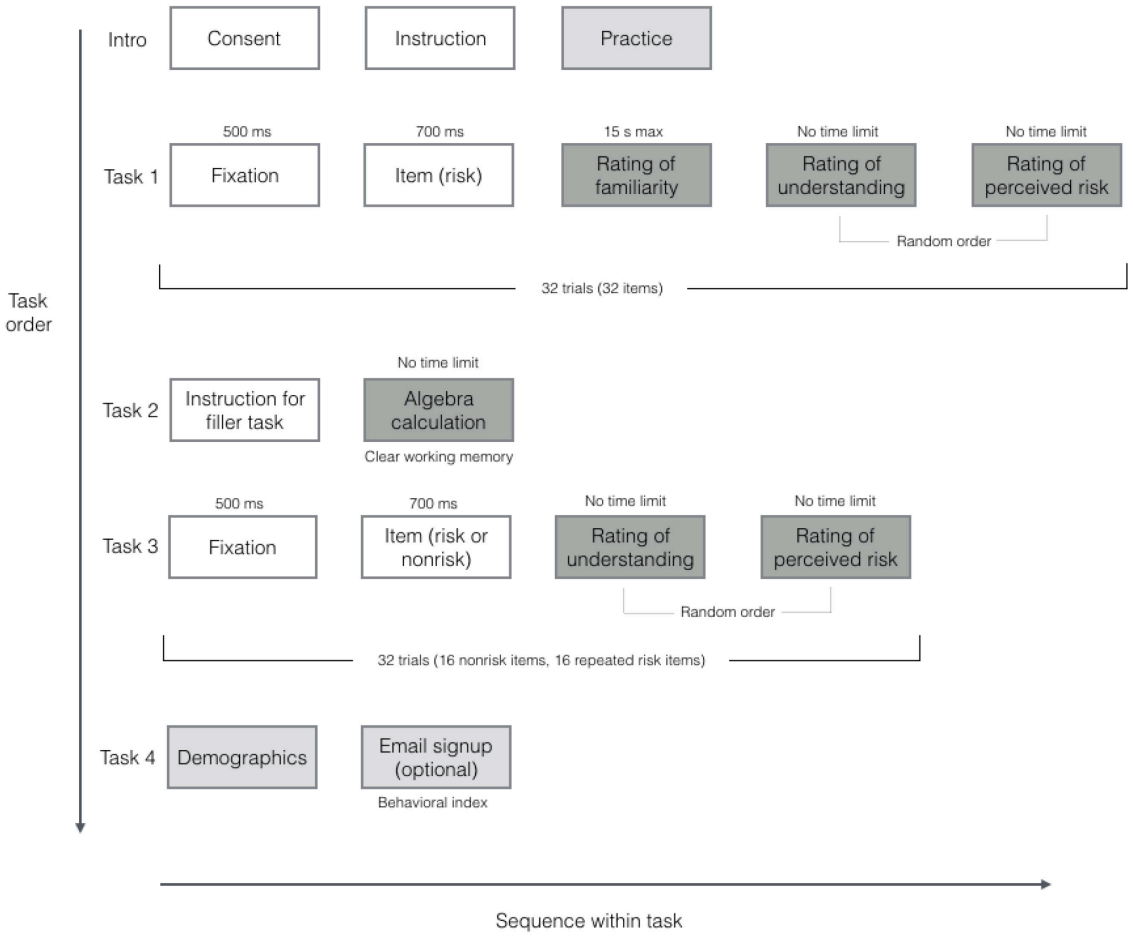


FIGURE 1. Illustration of experiment tasks for Study 1

After 32 trials (32 item presentations and 32*3 total numbers of ratings) were completed, the participants were instructed to finish a series of algebra calculations (task two), which is a common method to occupy human working memory (J. R. Anderson et al., 1996; Baddeley, 1992), thus preventing explicit memorization of the tested items and their own initial ratings. After all calculation tasks, participants had a short break, during which we expect they fully recovered from practice and fatigue effects.

Following the break was another rating task (task three), the structure of which resembles that of task one. However, the items presented this time were a mix of new and old. There were 16 randomly duplicated items from task one, but the other 16 were new items concerning general information technology topics not specific to ISec. The mixture of materials intended to further prevent the explicit memorization of ratings from Task 1, and it also served as a manipulation check, such that ISec threat items should yield more perceived risk than non-risk IT-relevant items. However, no rating of familiarity was required in this task since we already had the baseline and manipulated ratings for familiarity for all 32 threats from the previous block. This is to further remove potential influence of the "rating" of familiarity itself on the rating of perceived understanding and risk.

Finally, participants filled in demographics with questions asking if they have memorized their own ratings. Then they proceeded to the final page, where they submitted the experiment data to the server. On this same last page, we implemented an optional "email signup" checkbox with input field. They were told that if it is filled, they would receive a one-time-only email newsletter on practical tips and recommended techniques to achieve better online security. This served as a behavioral indicator besides the self-reported ratings of ISec threats.

2.4.3 Materials and Measurement

Based on previous ISec studies (Huang et al., 2010; Jeske & van Schaik, 2017; van Schaik et al., 2017) that directly address the measurement of risk perception and explicit construct of familiarity, we compiled a list of 32 common ISec threats (see Table 1). We supplemented them with explanatory information partly based on previous instruments (Garg & Camp, 2012; Huang et al., 2010; van Schaik et al., 2017), but mainly on explanatory information from top search results on Baidu, which is the dominant Internet search engine in China. The search results were largely from well-known public wikis and corporate websites. By using this information, we aim to render more practical relevance, as online search is one of the most pervasive and accessible information-acquiring methods.

TABLE 1. 32 common ISec threat items and explanations excerpted from most accessible online search results

Abbreviation	**ISec Threat Title**	**Explanatory Information**
BP	Backdoor Program	A computer program that gains unauthorized remote access to a compromised PC system.
BN	Botnet	A group of computers infected by malware and controlled by one malicious actor.
CF	Catfishing	Fabricating online identities and tricking people into emotional relationships to gain economic and informational benefits.
CT	Computer Theft	Physical theft of personal computers by thieves or other parties.
CK	Cookie	A small file stored on an Internet user's computer (usually encrypted), created and subsequently read by a website to track users and user settings.
CI	Copyright Infringement	Use of one's work published online, illegally and without permission.
CB	Cyber-bullying	Doing harm to individual or a group of people on the internet.
DW	Danger to Wellbeing Through the Use of Internet	Negative impact on human physical and mental health using the internet.
DS	Denial of Service	Any sort of attacks where the attackers attempt to prevent legitimate users from accessing service or resources normally accessible.
DQ	Deviation in quality of service from service providers	When service providers fail to manage data traffic on the network in any way.
EH	E-mail-harvesting	The process of obtaining many email addresses through various methods. The email addresses may be used later in bulk emailing.
HK	Hackers	Originally refers to a highly skilled computer expert. In media coverage, it usually means someone who uses bugs or exploits to break into computer systems.
HF	Hardware failure	Failure of computer hardware from natural degradation, corruption, natural disaster, or other causes.
IT	Identity theft on the Internet	Acts where someone uses another person's personal data to forge a false identity, such as Social Security Number, driver's license, and credit card information.
IA	Internet addiction	A mental state in which users feel a compulsive desire to surf the web after being immersed in online environment for too long.
IS	Internet surveillance	The monitoring of the online behaviors and activities in a local network.
KL	Keylogger	A type of spy software that records the user's every keystroke.

Abbreviation	ISec Threat Title	Explanatory Information
MW	Malware	Software between the virus and normal software, usually installed without the knowledge of the owner and undermining the user's legal rights.
OA	Operation accidents	Circumstances where human actions, decisions or behaviors cause ISec issues.
PS	Piratical software	Software copies distributed without legal ownership.
RW	Rogueware	Software between a virus and normal software, usually installed without the knowledge of the owner and undermining user's legal rights.
SE	Social engineering	The art of manipulating people so they give up confidential information during human interactions.
SB	Software bugs	Problems in which the faults in the program lead to crashing, glitching, data loss and abnormal interruptions.
SPA	Spam	Unrequested or unwanted emails in users' mailboxes.
SPO	Spoofing	A fraud in which communication is sent from an unknown address disguised as a source known to the receiver.
TA	Theft of account credentials	Any means by which a victim's proof of identity is stolen.
TC	Theft of credit card details	Any means by which a victim's credit card details are stolen.
TH	Trojan horses	A type of malicious code often hidden in legitimate software. It can be used to gain remote access to users' systems.
VS	Virtual stalking	Use of the Internet to stalk, follow, and harass another person.
VR	Virus	A malicious program implemented to infect the computer and user data, which is also capable of replicating itself.
WO	Worms	A common computer virus that copies itself from machine to machine via the internet, thus scanning and infecting increased computers.
ZP	Zombie PCs	Computers connected to the Internet that have been infected by virus, thus being taken over by hackers, proceeding to DoS attacks, and sending junk messages.

Two criteria for the compilation were the potential range of expected perceived risk and variety of threat types, for avoiding ceiling effect and a wider coverage of topics. It is also worth mentioning that some risks are more open ended, such as cookies, unauthorized use of software, (Fang & Lee, 2016) and internet surveillance (could be considered a protective means for national security or a danger to civil rights). We also included a threat named "danger to well-being through the use of the Internet" as an example of an intersection between physical risk and virtual activities.

2.4.4 Results

2.4.4.1 Manipulation Checks

ISec risks (simple: M = 5.10, SD = 0.81; informative: M = 5.05, SD = 0.47) were perceived as more threatening than non-risks as we intended (simple: M = 3.69, SD = 0.64; informative: M = 3.83, SD = 0.47), with $t(59) = 7.66$, $p < 0.001$ in the simple condition and $t(62) = 10.35$, $p < 0.001$ in the informative condition. We categorized ISec threat items into three groups based on the mean and the mean ±1 standard deviation, namely the high-threatening groups, medium, and low-threatening groups. Interestingly, 6 (simple condition) and 7 (informative condition) non-risk items were perceived as threatening as some of the ISec items. For example, in the simple condition, WeChat (M = 4.19) was perceived as threatening as those in the low-threatening group. Ride Share Service (M = 4.31), Baidu (M = 4.61), Chatting with Strangers (M = 4.65), Online Banking (M = 4.94), and Dark Web (M = 5.38) were comparable to those in the medium group. This has two implications. For one, people may be able to relate simple IT-related concepts to more complicated meanings underneath, even if it was only the bare mentioning of names. Further, even a visual stimulus as simple as a word may serve as a kind of fear appeal in some situations.

Towards the end of experiment, the program asked the participant to recall two ISec items presented during the study. Each of the 32 ISec items was recalled one to three times, which indicated the programmed randomization effectively reduced bias on attentive information selection. We also randomly conducted short after-experiment interviews on the memorability of the item ratings by asking the participants whether they remembered any of the ratings for any items from the experiment session. Out of the 20 interviewed participants, 18 reported that they could not remember any ratings. Two did claim they remembered some ratings, but report-data verifications showed their recalled ratings were not correct. This further supported the elimination of memory and practice effects.

Lastly, we address that there is no manipulation check of participants' subjective evaluation of the complexity of materials. That is, we did not measure whether the material in the simple condition is perceived as simpler than the material in the informative condition. There are two considerations in leaving out the implementation of such. For one, measuring the level of material simplicity was deemed as a redundant step that could easily have participants engage in more intentional processing of materials, and possibly in leading them to rate

their perception of familiarity, understanding, and risk, based on reflected information richness rather than natural intuition. For another, the purpose and inspiration of this experimental design, as described early in Section 2.4.3, is to draw a comparison to the scenario where people, whether by design or by self-choice, only receive minimal security information of titles and names, as well as the scenario where people are exposed to those most accessible descriptions of security threats on the internet that lay out the knowledge prompts compiled in the experiment. In this sense, the categorization of "simple" and "informative" condition is not an assumed statement on participants' pre-existing psychology, but rather nominal titles to classify our intentionally implemented experiment stimuli subject to interpretation.

2.4.4.2 Ratings for ISec Threats

We aggregated the data across 32 ISec threat items overall and for each, yielding the baseline familiarity, baseline perceived understanding, and baseline perceived risk ratings before the manipulation (repetition) phase. The descriptive statistics are listed in Table 2. Threat abbreviations are listed in Table 1.

Tables 3 and 4 show the correlation matrix among the main ratings tasks and corresponding reaction times. In the simple condition, rating of familiarity and rating of perceived understanding is highly correlated, $r(30) = 0.969$, $p < 0.001$. It indicates people may have based their perceived understanding on their feeling of familiarity. Familiarity and perceived risk are significantly and moderately correlated, $r(30) = 0.504$, $p < 0.005$, which supported that the participants may have rated perceived risk based on familiarity. For the informative condition, however, rating of familiarity was not significantly correlated with perceived risk anymore, which shows that participants rated risk based less on only familiarity and potentially took time to attempt to understand the written explanations of threats. Further, in the informative condition, the rating of familiarity was negatively correlated with the time it took to rate, $r(30) = -0.376$, $p < 0.05$, showing that the more time participants took to rate familiarity, the less they were likely to rate an item as familiar. Together, the results support that the informative condition did have behavioral effects in the way participants rated, if not on the rated value. Additionally, the rating of familiarity is also positively correlated with the reaction time of rating understanding in the simple condition, which we have not expected: $r(30) = 0.367$, $p < 0.05$. We interpret this data as people took more time to reflect whether they understand the names of threats which they claim as familiar.

TABLE 2. Ratings of familiarity, understanding, and risk of 32 risk-relevant threats at the baseline level (mean followed by standard deviation in parenthesis)

ISec threat	Familiarity (simple)	Familiarity (informative)	Understanding (simple)	Understanding (informative)	Risk (simple)	Risk (informative)
BP	2.88 (1.87)	3.24 (1.81)	2.92 (1.74)	3.18 (1.59)	4.2 (1.84)	4.36 (1.79)
BN	2.59 (1.60)	3.3 (1.89)	2.73 (1.67)	3.76 (1.97)	4.37 (1.39)	4.90 (1.82)
CF	5.55 (1.50)	5.47 (1.60)	5.43 (1.47)	5.18 (1.73)	5.1 (1.77)	5.10 (1.89)
CT	5.7 (1.76)	5.62 (1.76)	5.39 (1.78)	5.46 (1.69)	5.96 (1.41)	5.16 (1.93)
CK	4.51 (1.71)	4.22 (1.88)	3.88 (1.51)	4.32 (1.50)	3.88 (1.73)	4.48 (1.53)
CI	5.12 (1.42)	5.43 (1.66)	4.96 (1.46)	5.06 (1.57)	4.55 (1.58)	5.08 (1.70)
CB	5.41 (1.69)	5.42 (1.83)	5.43 (1.37)	5.04 (1.74)	5.29 (1.69)	5.08 (1.63)
DW	5.43 (1.21)	5.46 (1.39)	5.16 (1.32)	5.02 (1.46)	4.94 (1.57)	5.04 (1.76)
DS	2.14 (1.60)	2.88 (1.95)	1.96 (1.43)	3.12 (1.80)	4.04 (2.04)	4.70 (1.84)
DQ	4.43 (1.72)	4.79 (2.00)	4.37 (1.77)	4.50 (1.91)	4.24 (1.49)	4.18 (1.57)
EH	3.67 (1.80)	4.83 (1.79)	3.78 (1.68)	4.64 (1.84)	4.35 (1.68)	5.04 (1.63)
HK	5.18 (1.52)	4.94 (1.76)	4.43 (1.60)	4.52 (1.79)	5.43 (1.71)	5.10 (1.58)
HF	5.02 (1.76)	5.3 (1.80)	4.65 (1.57)	5.08 (1.59)	4.86 (1.44)	4.82 (1.65)
IT	4.78 (1.69)	5.27 (1.48)	4.73 (1.54)	5.06 (1.57)	5.76 (1.34)	5.92 (1.34)
IA	5.78 (1.42)	5.54 (1.75)	5.61 (1.36)	5.5 (1.62)	5.12 (1.76)	4.66 (2.20)
IS	5.02 (1.67)	4.96 (1.67)	4.61 (1.5)	4.48 (1.84)	5.12 (1.66)	4.90 (1.63)
KL	2.96 (1.87)	3.12 (1.89)	3.25 (1.89)	3.58 (1.83)	4.1 (1.88)	5.20 (1.85)
MW	5.62 (1.37)	5.09 (1.72)	4.78 (1.65)	4.84 (1.74)	5.92 (1.28)	5.68 (1.54)
OA	2.8 (2.02)	4.41 (1.99)	2.73 (1.89)	4.24 (1.84)	4.24 (1.59)	5.16 (1.60)
PS	6.18 (0.97)	5.36 (1.59)	5.41 (1.39)	4.92 (1.55)	4.16 (1.90)	4.70 (1.71)
RW	5.12 (1.85)	4.82 (1.92)	4.71 (1.90)	4.50 (1.90)	5.27 (1.73)	5.32 (1.43)
SE	2.2 (1.63)	3.57 (1.93)	2.37 (1.68)	3.70 (1.79)	4.57 (1.77)	4.78 (1.71)
SB	4.86 (1.68)	5.44 (1.64)	3.96 (1.68)	5.00 (1.46)	4.37 (1.67)	5.04 (1.75)
SPA	6.47 (0.86)	5.92 (1.48)	5.76 (1.57)	5.22 (1.82)	4.06 (2.03)	4.94 (1.65)
SPO	4.14 (1.73)	4.08 (1.99)	4.08 (1.47)	3.94 (1.72)	4.98 (1.49)	5.02 (1.60)
TA	5.76 (1.32)	5.39 (1.82)	5.35 (1.51)	4.96 (1.73)	6.39 (1.04)	5.82 (1.26)
TC	5.49 (1.39)	5.45 (1.83)	5.06 (1.67)	5.04 (1.74)	6.22 (1.29)	5.76 (1.64)
TH	5.22 (1.47)	4.82 (1.74)	4.24 (1.80)	4.08 (1.78)	6.02 (1.24)	5.66 (1.48)
VS	4.55 (1.63)	4.76 (1.62)	4.29 (1.50)	4.82 (1.69)	5.33 (1.45)	5.24 (1.86)
VR	5.45 (1.64)	5.18 (1.75)	4.9 (1.79)	4.82 (1.81)	5.98 (1.29)	5.68 (1.42)
WO	3.47 (1.89)	3.78 (1.86)	3.14 (1.82)	4.12 (1.90)	5.04 (1.81)	5.46 (1.69)
ZP	2.71 (1.68)	3.67 (1.87)	2.75 (1.68)	3.68 (1.63)	4.61 (1.63)	5.06 (1.75)

TABLE 3. Correlation matrix of baseline ratings and reaction times (duration) for the simple condition

F. rating	-0.099	-0.037	0.367*	0.504**	0.969**	1
U. rating	-0.008	-0.093	0.311	0.490**	1	N/A
R. rating	0.029	-0.343	0.307	1	N/A	N/A
U. duration	0.069	0.294	1	N/A	N/A	N/A
R. duration	0.162	1	N/A	N/A	N/A	N/A
F. duration	1	N/A	N/A	N/A	N/A	N/A
	F. duration	R. duration	U. duration	R. rating	U. rating	F. rating

F for Familiarity; U for Understanding; R for Perceived Risk

TABLE 4. Correlation matrix of baseline ratings and reaction times (duration) at baseline for the informative condition

F. rating	-0.376*	-0.326	0.128	0.290	0.957***	1
U. rating	-0.331	-0.334	0.128	0.278	1	N/A
R. rating	-0.142	-0.251	0.105	1	N/A	N/A
U. duration	0.010	-0.144	1	N/A	N/A	N/A
R. duration	0.297	1	N/A	N/A	N/A	N/A
F. duration	1	N/A	N/A	N/A	N/A	N/A
	F. duration	R. duration	U. duration	R .rating	U. rating	F .rating

2.4.4.3 Perceived Risk and Behavioral Coping

We aggregated the experiment data by participants in this section. We removed the ratings for ISec items that were not repeated in the repetition phase for each participant, then marked the mean ratings of their more familiarized items and less familiarized items. Next, we conducted ANOVA (with R 3.6.1 and its "ez" library Version 4.4) with communication "complexity" as a between-subject variable (simple vs. informative), repetition (i.e., manipulated familiarity), and baseline familiarity as within-subject variables in in a three-way mixed ANOVA analysis. The results are summarized in Table 5 and Figure 2.

TABLE 5. Mixed ANOVA results with data from Studies 1 and 2

Effect	**DFn**	**DFd**	**F**	**P**	**P < 0.05**	η_{ges}^2
Complexity (simple vs. informative)	1	99	0.194	0.661		0.001
Baseline Familiarity	1	99	38.988	0.000	*	0.051
Manipulated Familiarity (Repetition)	1	99	2.678	0.105		0.002
Complexity*Baseline Familiarity	1	99	1.987	0.162		0.003
Complexity*Manipulated Familiarity	1	99	4.112	0.045	*	0.003
Baseline Familiarity* Manipulated Familiarity	1	99	4.506	0.036	*	0.002
Study*Repetition*Familiarity	1	99	1.317	0.254		0.000

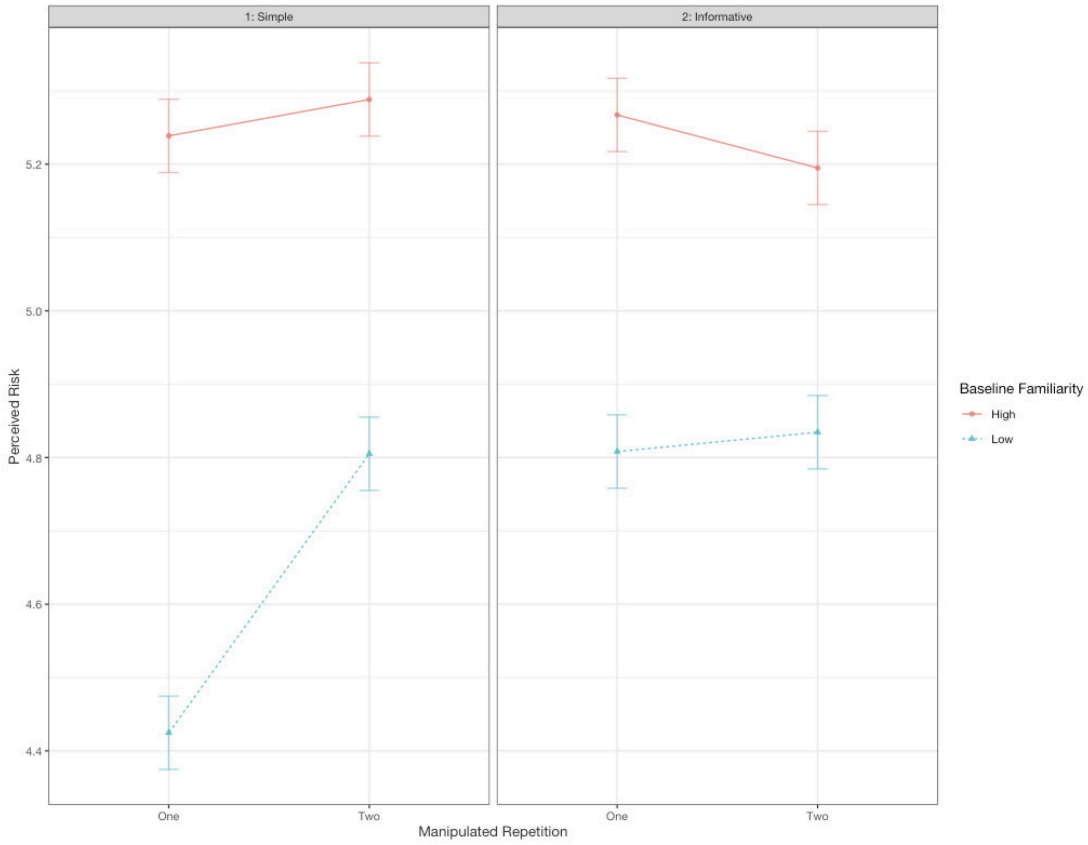


FIGURE 2. Perceived risk by baseline familiarity, manipulated familiarity, and communication condition (simple or informative)

While there was a significant main effect of baseline familiarity, main effects of communication complexity and repetition were not found. It suggests that, on average, higher baseline familiarity is correlated with higher perceived risk, but neither manipulated increase of familiarity nor explanatory information significantly affected perceived risk. However, there was indeed a significant interaction effect between communication complexity and manipulated familiarity, as well as between baseline familiarity and manipulated familiarity. It indicates that the manipulated increase of familiarity affected perceived risk in two complexity conditions in different ways. In the Simple condition, increased in familiarity led to higher perceived risk, but only for those ISec items with a lower baseline familiarity to start. In the informative condition, familiarity did not significantly affect risk perception, in spite that it affected the way participants rated the ISec threats as we discussed above.

Further results in behavioral coping reveals a somewhat alarming effect. In the simple condition, 29 of the 51 participants signed up for the email correspondence, but only 12 out of 50 participants signed up in the explanation condition, which is a significantly lower rate, $\chi 2(df = 1, n = 101) = 11.31$, $p = 0.001$. This shows that, as communication material became more informative, behavioral coping rate dropped while rated perceived risk maintained as comparable. On the other hand, manipulated increase of familiarity in the simple condition was able to raise risk perception at a similar level with the informative

condition with lower exposure rate, and at a higher behavioral coping rate. Manipulated increase of familiarity barely did anything for the informative condition where the level of risk perception is high to begin with.

2.5 Discussion

2.5.1 Contributions of Study 1

We defined, implemented, and manipulated familiarity experimentally for the first time for IS, aiming to study the effect of baseline familiarity (pre-existing familiarity towards ISec threats), manipulated increase of familiarity (increased repetitions of communication material) and material complexity (simple or informative) on persuasive results (i.e., perceived risk and behavioral coping). Our study offers three major new contributions and two minor contributions.

2.5.1.1 Major Contributions

Our first main contribution suggests divergent effects of repetition-based familiarity and the complexity of communication material (also an attempt to increase people's familiarity). The increase of manipulated familiarity, while increased perceived understanding, only raised perceived risk when the communication material was as simple as the short names. We see the raise in perceived understanding an "illusion of knowing", as it was unlikely that participants gained substantially more understanding from repetitive exposures during the experiment sessions. On the other hand, repeated exposures to more informative communication materials have decreased behavioral coping rate while maintaining perceived risk as comparable to that in the simple condition. We see this an alarming phenomenon where the superficial "knowing" is coupled with undermined "doing".

With regard to perceived risk, the data showed that repetition only increased the perceived risk for participants with a low baseline familiarity to begin in the simple condition. It suggests that familiarity may have a ceiling effect beyond which it does not have extra effects. However, previous research on repetition-based familiarity in psychology (see meta-analysis by Montoya et al., 2017) often found the effects of repetition on recognition and liking to reach their peak at more than 20 exposures, which is far more than our implementations of two exposures. This difference may imply two possibilities. First, while psychology used neutral and nonthreatening (e.g., neutral statements of facts) experimental materials, the effects of familiarity with socially threatening stimuli such as ISec threats may reach its peak earlier. Second, as psychological studies used dependent metrics such as perceived likeness and message agreement, familiarity may reach its peak effect much quicker with the metric of perceived risk. If the "liking" of something is in reverse relationship with perceived risk toward the same thing, it would be plausible that more exposures could lead to

decreased perceived risk and increased liking towards ISec threats in some conditions. Regardless, we have shown that the effect of specific familiarity varies based on the complexity of ISec communication and baseline familiarity level, which goes beyond previous implementations of general self-reported media exposure (C. L. Anderson & Agarwal, 2010; Chen, 2016) and "in-survey" familiarity (Alraja et al., 2019; Amran et al., 2018; Huang et al., 2007, 2010; Jeske & van Schaik, 2017; Nepomuceno et al., 2014).

The informative condition had behavioral effects on the participants in the way they rated metrics, with a negative correlation between the time it took to rate familiarity and the actual rating, as well as the absent correlation between risk rating and familiarity rating. They suggest that participants may have taken more time during rating familiarity reflecting written explanations, and they based their rating of risks less on familiarity and more on intentional reflections. However, the overall familiarity, understanding, and final risk ratings in the informative condition did not increase significantly compared to the simple condition, despite that the explanations raised rating of perceived risk at the baseline level (one exposure) to the level with two exposures in the simple condition. We address that the explanatory information was tailored from the most accessible information in top search engine results, which indicates the spread of prevalent information like this was very limited in achieving effective persuasive metrics. The negative result for post-task behavioral index furthered this limitation. With significantly fewer people signed up for email correspondence in the informative condition and the equivalent overall level of risk perception, people have engaged less behavioral coping while regarding the ISec threats as equally threatening on the surface, which, to us, is more alarming than a straightforward negative effect on both perception and behavior.

Overall, our first contribution questions the efforts in raising people's familiarity with ISec threats with repetitive exposures and presentation of popular online knowledge. We have showed that behavioral coping could decrease even when perceived risk stays the same, which may imply a knowing−doing gap (Cox, 2012) where a superficially sufficient level of "knowing" could lead to decreased "doing".

The second main contribution comes from our emphasis on both the general and the specific. Some IS security scholars have recently noticed the importance of context specificity recently (Aurigemma & Mattson, 2018; Siponen & Klaavuniemi, 2019). We showed that repetitively presenting ISec threats with simple and more informative forms could result in varied relative rankings in people's perceiving 32 ISec threats, while the average rating of familiarity and perceived risk stayed the same. For example, "pirated software" was perceived as one of the most familiar and ominous threats when only the name was presented. However, both its relative ranking and absolute rating decreased in the informative condition. The reverse is true for other threats, such as "software bugs". Our findings here are new and important, suggesting that the same kind of manipulation could yield different results for individual risks, while the average metric stays the same. Meanwhile, it also implies potential solutions to

tailor ISec communication exposures and complexity for different individual ISec threat types.

Third, we also consider our adaptation of the psychological experimental method (Garcia-Marques, 2000; Garcia-Marques & Mackie, 2001; Moons et al., 2009) as a contribution to IS. The implementation of an experiment allows the inference of causal relationships and precise control of variables (Leik, 2013). The experimental nature of our design allowed us to explain the correlation matrix table of main rating metrics in a causal fashion. We also utilized standard experimental design strategies in psychology (Tanner, 2002), such as stimulus randomization and distraction tasks (i.e., arithmetic calculation) to reduce practice effect, order effect, and fatigue (Grant, 1948), which may be hard to control in traditional surveys. We utilized the experiment programming tool Lab.js (Henninger et al., 2019), to implement experiments on modern web browsers and record precise metric such as the reaction time for rating, which is a common metric in psychology and communication studies (Allen, 2017, p. 1045).

2.5.1.2 Minor Contributions

We contribute by offering descriptive results of folk perception for common ISec threats. While the degree to which these ratings of perceived familiarity, understanding, and risk were "rational" enough may be up to more authoritative evaluations, the data could be helpful for practitioners concerning policymaking and resource allocation to where the awareness is still lacking. Our sample is a meaningful addition to previous research that studied similar ISec threats and constructs with nonexperimental measurements (Garg & Camp, 2012, 2012; Huang et al., 2007, 2010; Jeske & van Schaik, 2017; van Schaik et al., 2017) and further comparisons could gain insights into the similarities and differences in different samples and cultures. For example, compared to Jeske and van Schaik (2017), our sample is much less familiar with "cookies." This may be because popular computer operating systems (e.g., Microsoft Windows 7 with the Chinese language pack) only use the English term "cookies" without translating it into Chinese.

Moreover, we included more varieties of ISec threats compared with previous survey studies (Garg & Camp, 2012; Huang et al., 2007, 2010; Jeske & van Schaik, 2017; van Schaik et al., 2017). Our materials included more varieties of ISec items with risks extended to the virtual−physical (e.g., rideshare service) and psycho−physical (e.g., mental wellbeing issues using the Internet) sphere other than virtual-only risk, which yields interesting comparisons. For example, the data suggested "computer theft" as perceived more threatening than "identify theft," while "ride sharing" (one of the non-target items) seemed equally threatening as traditional ISec risks such as "keyloggers" and "botnets." In addition, a few "non-risk" items, such as WeChat and Baidu, were perceived as equally threatening as some of the "actual" ISec risks even in the simple condition. While the interpretation of these results remains open, we argue that ISec risks encapsulate more complex implications as socially constructed

concepts themselves, and the bare mentioning of ISec threat names could already incite other connected thoughts as mental reference.

2.5.2 Implications for Practice

Our results offer practical implications for existing ISec communications, such as fear appeals. For ISec threats with which people are still not familiar, we suggest moderately repeated social campaigns that incorporate less knowledge-based information to simply promote familiarity while bringing the topic to public discussion, as it may be already enough to raise perceived risk and maintain a fair behavioral coping rate. For ISec threats with which people are already much aware, campaigns that only highlight simple information may not work anymore. However, if the campaign intends to convey more complicated knowledge to communication recipients, the issuer should be careful with the choice and design of information, since if not produced well, they could further decrease behavioral coping rates while maintaining the comparable level of awareness and perceived risk on the surface. In addition, web content providers should note that some of the most accessible information online about ISec threats could undermine actual risk coping performance.

For more implications, a one-size-fits-all campaign strategy may yield different persuasive results for specific ISec threats. The choice of materials which encapsulate similar or connected ISec threats (e.g., spam and email harvest) also entail different results, thus requiring varied explanatory supplements. Even if the average persuasive effect does not vary for a cluster of threats, there may be relative difference for individual threats. Smart communication design should consider the classification of threat clusters, based on which to work towards different levels of intended communication familiarity and complexity. Lastly, as our choice of communication context is only one of many possible scenarios, we encourage readers to interpret the results flexibly, and combine their experience for ISec communication implementation.

2.5.3 Potential Limitations and Research Directions

It may be argued that our experimental method is lacking in ecological validity (e.g., the kind of textual material we implemented would not appear in real organizational settings). However, we would like to remind readers of this study's purpose and the experimental method we migrated from psychology.

First, our interest has not been in organizational contexts from the beginning, where information of threats is often wrapped, discussed, and applied in company policies, employee roles, and work guidelines. As introduced early in the writing, we are interested much more in daily settings where familiarity come from intentional as well as unintentional sources even if a threat's name is just a mention in a casual conversation. We deem this important and overlooked in IS, because it is the citizens' collective attitude and action that receive and feed back to how media contents, technological products, and services designed for the public. Second, to our knowledge, this study is the first experiment in IS

dedicated to the concept of familiarity. The exact statistics in absolute number is secondary to what we can demonstrate better, which is the variance of the effect of familiarity as an independently manipulated variable on risk perception and coping, as well as that its effect can be differentiated for different types of threat. In essence, we would like to present an empirical to make a point in urging the contextualization in the field of familiarity and media presentation formats, if not also for the study of many more mental constructs in MIS.

Furthermore, we reason that while our study is the one of the first that introduces this experimental method to IS, it would be better to keep the original form of design and control, so that future studies may have a concise design to build upon. We encourage future research to present organization-relevant stimuli with our frame of design, such that the texts could be tailored excerpts from actual company policies. But again, this has not been our interest from the beginning. Also, we would also like to add that the potential problem of the lack of ecology can be also true for survey studies which involve written questions and constructs detached from real-life. In our study, efforts were at least made to greatly reduce practice effects and demand characteristics with the accurate manipulation of independent variables, which is not available to traditional surveys. For us, the variety of contexts lies in our implemented collection of ISec threats and manipulation of repetition and information richness, which conceptually approximate different sources of familiarity and overlooked ISec communication scenarios in real life. We reckon that experiment-based studies have much advantage in precisely manipulating a few variables and serving as accurate research prototypes for larger scale practice. For the topic of familiarity, future research could implement different variations of security communication formats, information richness, stimulus repetition range, rest periods between repetitions, and more ISec threat scenarios with similar experimental method we propose here.

Another limitation regards the complex and nonuniform nature of the ISec materials. For example, when compare "theft of credit card details" with "virus," the former was perceived as more threatening among the threats tested, but we cannot be sure if it was the threat per se that yielded this difference. Because the linguistic saying of "theft of credit card details" already emphasizes the outcome of security risks, as opposed to the simple word of "virus". However, this limitation was also shared by previous research, and critical minds should further ponder if it is even possible to denote an ISec threat without emphasizing a particular linguistic facet. For this, studies on the naming and linguistic structure of ISec threat titles, along with their effects on risk perception, should be encouraged in future research. Further, it may be also for this reason, that readers may consider it not proper to pool average date across all 32 topics used (e.g., average perceived risk across topics). However, with the rationale stated just now, we would like to address two points. First, the introduced experimental method allows homogenous or heterogenous materials to be used in future research, which shows its own value and contribution to the research field. Second, and also more critically, we must ask what would be the nature of a general evaluation of people's perception of security threat, if it is not composed

of a range of diverse threats averaged in pool? It would be possible, for instance, that individuals use a separate mental impression to evaluate the general concept of threat, rather than performing a rational calculation that averages different types of threats (in thinking so one has to criticize many foundational economic models that assume the nature of a calculative human decision-making process), but our result of average risk perception is not only for possibly approximating the nature of collective psychology, but also for establishing a midline that separates highly perceived threats apart from the not-so ones, in order to make the point for promoting context-specific communication designs.

The last potential limitation we see regards the use of email signup as a measure of coping behavior. It is possible that participants only decided to sign up or not sign up based on if they want to *know* more about security threats, in which case it could explain why the people in the informative group showed lower signup rate (i.e., they have been exposed of enough information with no desire of getting more). For this, we would like to address the difference between the presented stimuli and the prompted content of the email correspondence. Our selected stimuli, as showed, are informative words or short definitions with no complete arguments or instructions. They do not explicitly suggest or not suggest any coping methods. The description of the email signup option though, as written in Section 2.5.2, was a one-time-only newsletter on *practical tips* and recommended *techniques* to *achieve* better online security, which clearly points to a functional purpose in practice. In addition to this, our setup is not contradictory to our initial interest in the daily scenario where one first gets familiarized with a threat randomly in life and later needs to make a certain decision related to this threat.

With this said, we still see other possibilities. First, the participants may have ignored the meaning of the prompt and in actuality decided to sign up based solely on the need for information. Or, they have just had enough of the threat information exposed and not wanting more of those, which may be postulated as due to security fatigue (Cram et al., 2021; D'Arcy et al., 2014) that we have discussed and compared with familiarity in Section 2.3. This is deemed not likely though for several reasons. First, the participants were not able to recall which items were actually presented twice and what their ratings were in the post-interview. Second, the use of the algebra test in between experimental blocks should in theory have cleared their working memory, and our experimental task in no way tested the participant's action conformation, memory, or skill, which should not pose unnecessary pressure. Third, even if some kind of fatigue happened, it should more "information fatigue" rather than "security fatigue", as the stimuli were not persuasions of security requirements, but only stated definitions of security threats and IT-related concepts. Hence, since the task is not framed in any way as pressure-inducing, we also deem this possibility unlikely.

2.6 Conclusion of Study 1

Our study offers three major and two minor contributions to the ISec literature. The main findings suggest divergent effects of the increase of repetition-based familiarity and information complexity for ISec communication. While the increase of familiarity has a limited positive role for perceived risk of ISec threats with low baseline familiarity presented in simple materials, it also led to undermined behavioral coping rate while keeping a superficial level of perceived risk. Methodology-wise, our study incorporated various types of ISec threats and demonstrated a new way for studying and manipulating psychological constructs for behavioral ISec research. As a final highlight, we would like to mention Deboard's visionary proposal (1994), in which the modern human can see experiences as either directly lived (e.g., personally experienced the consequence of password theft) or viewed through spectacles (e.g., getting to know about a threat and its consequence from an ISec campaign). With our results, it seems that some communicative spectacles could alarmingly lead to negative effects while maintaining a positive face value.

3 STUDY 2: RETHINKING "FEAR" APPEAL FOR ISEC COMMUNICATION RESEARCH: A MULTIFACETED EXAMINATION OF FEAR

For Information Systems (IS) Security research, fear appeal has become a common approach to promote security-related behavior. However, much remains to be discussed concerning the variety and qualitative nature of the concept of *fear* itself in information security (ISec) communication. The fear for ISec threats, as we argue, is a multifaceted construct that implies varied characteristics in different contexts. However, most studies seem to assume only the quantitative differences of "fear" without concerns for the quality underlying this linguistic label. Further complication to fear comes from its first neural measurement in MIS, as the results suggest a lack of fear in the perception of ISec fear appeals. We attempt to resolve inconsistent research results on the study of fear by discussing how fear can be characterized differently at the neural, experienced, and behavioral level. We acknowledge different priorities in defining, measuring, and implementing fear for IS research. Finally, we conclude our arguments with the importance of "consistency" in the conception and implementation of fear under IS contexts of complex differences. With our discussions, we open up opportunities in fear and general affective research for IS, which implies unique mental benchmarks potentially different to those found in psychology.

3.1 Introduction to Study 2

Fear appeal is a recognized approach for promoting security behaviors (Tannenbaum et al., 2015). Typically, in Information Systems (IS) Security, fear appeals are written statements describing the risk of IS security threats and recommended coping methods, aiming at promoting security relevant intentions, attitude and behaviors (Boss et al., 2015; Johnston et al., 2015; Johnston & Warkentin, 2010). Although fear arousal is considered to be important in

implementing such statements, the effect of fear is said to potentially *backfire* in some cases as well (Boss et al., 2015; Wall & Buche, 2017), leading to undesirable coping modes and exposure to even more risk (Ruiter et al., 2014). Further, evidence from neuroimaging technique has cast doubt the actual existence of fear in the perception of fear appeals and more general information security communication (Warkentin, Walden, Johnston, et al., 2016). Such findings urge IS community to further understand the puzzling role of fear, as well as other emotional constructs, in behavioral IS security. In this study, we raise the question of *whether IS community is talking about the same "fear" in these studies.*

We argue the use of the same word "fear" could mean very different scientific notions, and the fear experienced in different settings have varied qualitative characteristics. However, while IS scholars encouraged IS research to measure fear (Boss et al., 2015), commonly available measures, such as Likert scales, often aggregate fear into a single numerical record representing its intensity (see Appendix A of Moody et al., 2018 for typical measurement) in regression models. When considering why the persuasive effects of fear differ across studies, we concentrate on fear's decrease or increase in intensity (Wall & Buche, 2017, p. 286), but rarely consider its potentiality as a multi-faceted construct (Crossler et al., 2013, p. 93).

While IS security research has not paid much attention to qualitative differences of fear, understanding them could lead to theoretical and practical advancement. Despite that studies in psychology often considered self-reports to be the most sensitive measure of fear (Mewborn & Rogers, 1979; Ordoñana et al., 2009), IS study which incorporates physiological techniques may skip self-report and measure metrics such as blood pressure and brain activations. For example, the strongest argument *hitherto* that doubts the role of 'fear' in IS security is the absent evidence of fear in the pioneering fMRI (Functional Magnetic Resonance Imaging) study on the neural correlates of information security perception (Warkentin et al. 2016). At the same time, autonomous physiological metrics such as fMRI has been championed as more objective and accurate than self-reports (Brinton Anderson et al., 2016; Crossler et al., 2013). But what if people report a certain level of fear but we cannot identify any trace of fear from brain scans? Is there a possibility that we have found a new type of fear with a different neural activation pattern, or should we keep assuming that fear instances of different risks share the same measurable neural foundation?

For sincere yet stimulating discussions of fear, we refer to studies in psychology ranging beyond topics in health psychology that IS often cites, which greatly support our proposed qualitative variability of fear across contexts. Our critical reflections of fear are organized as follows. In Sections 3.2–3.4, we address the relationship between fear measured with self-report as well as with neuroimaging techniques, addressing the lack of a stable and one-to-one relationship between them. In Sections 3.5 and 3.6, we propose different priorities in defining and implementing fear, which bears flexible qualities and meanings across contexts. Finally, in Section 3.7, we discuss the key importance of maintaining contextual consistency in different streams of IS research on fear,

while overcoming the view of affective factors as clear-cut variables in theory and practice.

3.2 Fear and Some Fundamentals of the "Objectivity" of NeuroIS

The field of NeuroIS, which often utilizes neural measurements as indicators of mental constructs, has specific importance for the research of fear in IS. On the one hand, perhaps the strongest challenge to 'fear' (Warkentin et al. 2016) currently comes from NeuroIS research. On the other hand, NeuroIS is sometimes advocated to be able to offer objectivity measures in scientific writing and practice. In this study, we first raise the basic question whether NeuroIS can offer us the objective measure IS scholars sometimes associate to it (Sections 3.2.1 and 3.2.2). Only after we critically view those claims, aptitudes, or implications, we may then possibly see how fear can manifest differently across measurements (Section 3.4).

3.2.1 On the Promise of NeuroIS and Neurosecurity

While neuroscience and psychology developed approaches to identify biological foundation of emotions through measured autonomous activation patterns, this method has been adapted in IS for over a decade (Riedl et al., 2017). For IS security, physiological and neural measurements have been applied recently with a few pioneering studies demonstrating its potential in fear (appeal) research (Amran et al., 2018; B. Anderson et al., 2018; Crossler et al., 2013; Riedl et al., 2017; Vance et al., 2014, 2018; Warkentin, Walden, Johnston, et al., 2016). These studies use EEG (e.g., Vance et al., 2014), eye tracking (e.g., Brinton Anderson et al., 2016) and experiment-based fMRI scan (e.g., Vance et al., 2018), among other physiological indicators. All of these are dubbed 'NeuroIS' (Riedl et al. 2017), although eye tracking data may not be viewed as directly an indicator of "neural" measurement.

Here our focus is on one stream of the NeuroIS, sometimes called neurosecurity (Anderson et al. 2015; Brinton Anderson et al. 2016). As the name implies, neurosecurity studies use neural measurements as proxies of security-relevant constructs to study IS-security-relevant problems. These studies usually involve the implementation of a specific type of bio-signature scan while instructing participants through a range of behavioral tasks (very often participants are situated in machines stationarily while certain physiological marks being scanned). During analytics, then, the correlative data between bio-signature results and behavioral benchmarks serve as important basis to draw research conclusions. In IS security or neurosecurity literature, the neural approach is often championed as more superior to traditional self-report measures, which is reflected in research writing and potentially in shifted future direction of the field. For example, Crossler et al. wrote

> For information security fear appeals to be effective, however, the appeal *must* successfully *manipulate* the neural regions of the message recipient's brain responsible for cognitively processing perceptions of threat and efficacy. (Crossler et al., 2013, p. 93)

Vance et al. note how

> Risk perceptions are often associated with feelings—such as fear or doubt—that are difficult to measure *accurately* using survey instruments. Additionally, it is unclear how these self-reported measures *map* to actual security behavior. (Vance et al. 2014, p. 679)

As a final example, Brinton Anderson et al. wrote

> NeuroIS holds the promise of 'providing a richer account of user cognition than that obtained from *any other source*, including *the user himself*' (Minnery & Fine, 2009, p. 73). (Brinton Anderson et al., 2016, p. 366)

In summary, the IS security literature often portray the neuro approaches as more accurate, objective, representable and capable of pushing us closer to the "truth" of fear. A comment on whether we are justified in believing this, or if a better way to understand this, will come later. For now, we review what neuroIS suggests about 'fear'.

3.2.2 Fear and Neurosecurity

Warkentin et al. (2016) found no evident fear in the fMRI-based neurosecurity study. In the experiment, they presented participants with short IT threat statements, such as "your data are in danger of being stolen" (Warkentin, Walden, Johnston, et al., 2016, p. 211), while scanning their brain activations with fMRI. Questions on message agreement, risk severity and susceptibility were administered at the time of performing scans and also after the stimuli exposure period. With the primary indicator of fear being activation of the amygdala, it was found that company employees showed no significant activation in this area, which was further interpreted as the evidence that fear was not invoked when exposed to security threats (Warkentin, Walden, Johnston, et al., 2016, p. 203). Moreover, the participants did not even show any clusters of activation in the limbic regions, which was interpreted as the evidence that IS security threats lead to little emotional consequence of any kind (Warkentin, Walden, Johnston, et al., 2016, p. 205). Overall, the results pose a doubt on those who advocate the role of fear (e.g., Boss et al. 2015).

While it would be possible that the participants did not find the messages threatening at all, hence producing no fear (this possibility is discussed in Section 3.5.2), we would like to ignore that possibility for now, and ask the following questions: is it possible to cognitively regard something as a threat without subjectively feeling it as in a way fearful? Do the neurosecurity studies warrant the superiority and objectivity that is sometimes alluded to them (Section 2.1.)? To what extent do the results like those just mentioned justify that no actual fear is elicited by fear appeal or other IS security communications? We address here that these questions are not asked only regarding Warkentin et al. (2016) but

proposed for NeuroIS studies in general. Attempts to resolve them is both meaningful to envisage a more probable explanation of fear for IS, as well as pushing research boundaries even when neural activation of IS metrics is not found.

3.3 The Alleged Objectivity and Accuracy of Neural Fear

3.3.1 On the Matters of Objectivity

As noted, cited studies in Sections 3.2.1 and 3.2.2 render neural measurement of fear as more objective. However, we consider the other possibility here, where neural measurement is not the objective and accurate method, and the adoption of them may veil a greater problem if we do not address the underlying issues. First of all, it is necessary to ask: what objectivity or "more accurately" means? It is important to discuss this, as something does not turn to being "objective" or "more accurately" with only a saying or it being physiologically measured. Alas, existing neurosecurity studies championing or hinting neuroIS as more objective or accurate does not say what makes them objective or accurate. Such unclarity can be problematic first because readers can ascribe different meanings to concepts, "with the risk of ending up with as many meanings as there are" (Rivard 2014 p. vii). Second, we may believe that something is self-evident, but when we open up the claim in detail, we may find it far from being self-evident.

What could objectivity mean? For example, one could claim the objectivity of neural measurements of fear in the way that they are observable and standardizable via mathematical aggregations of physical and physiological parameters. But self-report measures are also observable and standardizable, so saying this does not do the trick. Another way is to argue that self-reported measures are open to interpretations and biases, while neuroIS measures are not open to these. And for that reason, the argument continues, they are more objective and accurate. The general concern on objective observation is well-known in the philosophy of science under the tenets of theory-ladenness of observations (Hanson 1958) and underdetermination (resulting from Quine 1953 second dogma of empiricism). Theory-ladenness of the observations means that two different scholars may observe two different things based on their background. For example, the same microscope observation has been reported or interpreted differently based on scholars' background assumptions, or the meaning of observation can change over time, when the background information change (Siponen & Klaavuniemi 2021). Having said that, alluding to theory-ladenness of the observations only warn us that any observation may not be objective after all. Such generic tenet alone does not tell what aspect of fear the subjective "fear" in neuroIS could be. What then challenges the objectivity of fear?

One important factor is the instability of neural patterns of emotion and fear, which is relevant in understanding the relationship between measured fear in the brain and self-reported fear. Before looking at this, it is necessary to consider two

possible misinterpretations IS researchers might have if plainly accepting the arguments of static fear measurement standards. First, they may form the impression that different phenomenological feelings (e.g., reported fear or fear directly felt by human) are mapped with different biological signatures (e.g., specific brain activation patterns in fMRI). Second, they may also consider that commonly spoken typology of emotion (e.g., fear, happiness, sadness, as existing in daily language) corresponds to distinctive neural patterns. Subsequently, as long as these biological signatures (e.g., activation vs. inactivation of the amygdala) are identified, they may justify the legitimacy of claiming the occurrence of emotions even when people subjectively do not feel or report fear. Or the other way around, which is more relevant to current discussion, they may believe emotions do not exist "for real" when such neural patterns are not observed, perhaps even when people report fear to an extent on paper.

3.3.2 The Complexity of Neural Correlates of Fear

To put the thoughts in perspective, we start by briefly introducing two fundamental views of the human brain, namely the modular brain hypothesis and the distributive brain hypothesis (Okasha, 2016). With the modular view, the brain functions with a number of specialized sub-systems (modules), each of which has a specific purpose. With the distributive view, the brain is a general-purpose problem solver where all matters are processed in a highly distributed way. Empirically, both of them can be true to an extent. Research could indeed, identify certain neural activities in localized areas that exhibits predictable pattern correlated with behavioral tasks. For example, the MT/V5 area was once argued to be correlated with the processing of certain simple information of visual motion (Pollen, 1999, p. 5). Inferotemporal cortex was argued to respond selectively to visual shape features and subjects (Brincat & Connor, 2004, p. 880). However, this more straightforward correlations may be true only for very basic perceptive functions, and even for these, the identified brain sub-areas usually work in coordination with each other in complex dynamics (e.g., see Figure 1. in Pollen, 1999, p. 5). When we consider the cognitive function of visual mental imagery as a whole, it requires large networks of brain areas from frontal and parietal regions to the temporal lobe including not only bottom-up (e.g., pre-existing subjective thought affecting the processing of visual stimulus) but also top-down (e.g., features of visual stimulus decidedly affecting the activation of brain locations) processing (Bartolomeo, 2008; Mechelli, 2004). It is more likely that phenomenal experience of conscious perception in general involves a widespread network of brain area (Christensen et al., 2006). A broad review of neural correlates of human perception is not the scope of our study, but just as a recent methodology study in IS suggested, the more complex cognitive and affective processes in IS contexts, especially those involving decision-making, the more likely various activities in a network of brain regions are functionally integrated (Hubert et al., 2017, p. 9).

Specifically, for high-level mental construct as emotions (perhaps even more so for emotion episodes during decision-making process), its biological

signature does not really manifest in the measurement of specific and clear brain activation patterns (Clark-Polner et al., 2016). The multidimensional processing in amygdala could enlist many social and non-social representations (Gothard, 2020). While some research associated fear with the activation of *amygdala* with good rationale (e.g., Kim et al., 2011), especially those using animal subjects (Janak & Tye, 2015; Olucha-Bordonau et al., 2015), amygdala's activation is not really specific to the emotion of fear for human, but could be related to a wide range of psychological episodes as long as the stimulus are considered to be *motivationally salient* (Janak & Tye, 2015; Lindquist et al., 2012). Under this vantage point, stimulus designed to generate fear usually also attract greater attention in the audience, in which the associated physiological change both serve as the benchmark representing attention arousal as well as fear arousal (Ordoñana et al., 2009). For example, the activation of amygdala are correlated with both fearful and rewarding environmental stimuli (Gothard, 2020, p. 4; Janak & Tye, 2015, p. 284), and it could respond to many types of visual emotional stimuli regardless of their being positive or negative (Sergerie et al., 2008). Conversely, though increased amygdala activation may be more stably correlated with physical fear that involves physical freezing and potentiated startle, or what many refer to as the "fight-or-flight" response (see Milosevic, 2015 for an integrated view of fight-or-flight and freeze), not all *instances* of experienced fear are accompanied by increased amygdala activity (Suvak & Barrett, 2011). For instance, threatening contexts *devoid of salient visual stimuli* was found to elicit deactivations in the amygdala (Wager, van Ast, et al., 2009; Wager, Waugh, et al., 2009). Even in some psychological studies adopting fearful visual stimulus, amygdala did not show an increase in activation (Suvak & Barrett, 2011, pp. 6–7). It seems emotional experiences, particularly that of fear, does not correlate with the activation of one single decisive indicator, neither does the lack of activation indicate the definite lack of fear.

3.3.3 Further Evidence Against the Onefold Fear

Even by stepping back further and classifying emotions into only two broad categories, namely the positive or negative ones, empirical studies have supported the *affective workspace hypothesis*, suggesting that our precepted negative and positive valence cannot be relocated into clearly locational distinctions within the brain (Clark-Polner et al., 2016). In addition to the brain (part of CNS, the central nervous system), emotions are often studied together with the dynamics in the autonomic nervous system (ANS), which consists of the sympathetic nervous system (SNS) and the parasympathetic nervous system (PNS). Commonly measured indicators are heart rate, cardiac output, diastolic blood pressure, systolic blood pressure, respiration rate, and skin conductance response. However, very early fear appeal study (from the proposer of PMT) had already suggested that physiology changes of cardiovascular and electrodermal activities were not associated with attitude change, and that self-reports were the most sensitive measure of fear (Mewborn & Rogers, 1979; Ordoñana et al., 2009). Fear appeal research has argued that identified psychophysiological responses

came closer to a complex pattern related to *increased attention* than classic fight-or-flight response of fear (Ordoñana et al., 2009), the message of which resembles what we just discussed about amygdala. Recent comprehensive reviews in psychology further suggest substantial variations in different signatures of ANS activities within the same emotion category (Clark-Polner et al., 2016; Siegel et al., 2018). For example, the same threat may lead to response prone to fight, flight or freeze, depending on if there is external support and individual's experience with the threat over time, and they may *each* show a different kind of physiological response (Bradley & Lang, 2007). On the behavioral level, we may observe that people evade risk immediately in urgent cases, but they could also take time to be more thoughtful and reflective in others. With this level of complexity in emotional experience and biological signatures, it seems no on/off status of one or even a few selective physiological measurements could represent the holistic feeling people directly experienced at the moment.

In summary, fear does not correlate with the activation of one or a few decisive neural indicators, neither do the lack of activations indicate the definite lack of fear. Thus, neurosecurity observations hardly can be used to verify or falsify users' fear experience in a straightforward manner. However, we have arrived at a new problem at this point, which is the *contrast* between the linguistic label "fear" and correlation patterns of fear on the neural level. If we were to leave room for the possibility of predictable patterns from subjective experience to observable physiological activation, we need to further explore how the same use of "fear" to encapsulate instances of experiences may be different in the phenomenological world. That is, fear as a complex construct and what it means for IS, NeuroIS and ISec research.

3.3.4 Fear as a complex construct

As Barrett (2009, p. 1301) wrote, *very few people would deny the variety in emotional life*. Let us consider two instances of "fear" as examples, specifically, the "fear of being stalked". In the first example, one experiences fear of being stalked while realizing a stranger following her way home. In the second example, one experiences fear when realizing her being tracked online by an anonymous social media user. In the first case, we may imagine the person experiences sudden physical arousal, such as faster heartbeat and higher blood pressure. She might recall visuals from thriller films mentally, flashing back and forth. But she might also, at the same time, consider the possibility to physically confront the stalker, gauging what personal belongings of hers could be used for self-defense. She starts to remember a self-defense video while reaching her right hand to her mobile phone in the purse. In the second case regarding online stalking though, we may equally be able to imagine the same person just finding out someone has been stalking her online, while she experiences the fear of privacy compromise, as the virtual stalker may use the exposed information to phishing purposes, blackmail, or digital identify theft. She gets puzzled as not certain of the actual purpose of the stalker. Regardless, she turns on her laptop and feels that she should just block this user on social media first. But all of a sudden, she recalls

an old experience of being stalked one year ago on her way home. Maybe these two incidents are connected, the thought of which frightened her, leaving her unable to move for a moment, on her chair at her own home…

The previous "story" has been intentionally written to show the same person experience fear at two points of time with varied details. Even when she realized the connection between virtual stalking and physical stalking, her fear and the specific immediate physical response was not experienced in the same way. Many questions can be considered when we attempt to find an accurate measurement of her fear. Which single physiological arousal of them was the real or the best measurement of fear? At which time point should we measure an emotion indicator that represents the average fear the best? Was there a hidden constant factor across her mental feelings and physical expressions in the two instances that can be called fear? Was any part of the experience she had during the entire time closer to the true notion of fear, or should she herself regard the entirety of the experience as linguistically labeled as "fear"? For researchers, should we aggregate her neutral activations, record her physical behaviors, or just have her report her experienced fear retrospectively while "blindly" trusting her own recall of past emotions? With these questions, one may realize the differences and complexity in experienced fear across conditions. We argue that at least a set of factors, such as threat intangibility, physical immediacy, potential coping methods available, memory resource, and numerous other conditions specific to the risk context, hold together the uniqueness of very different fear-inducing situations, with fear experiences in parallel with changing thought processes, feelings, physiological activations, and potential neural activation patterns. However, such complex syndromes can all be linguistically labeled as "fear" and the contexts can be all regarded as "fear-inducing".

Our discussion does not imply that no patterns of neural activation can be observed during an *emotional episode*. More likely, it suggests that brain patterns observed along with different emotion categories or within different instances of the same emotion category (e.g., fear of being hacked and fear of spilling coffee on laptop) does not reflect neural foundation of any pure emotion, but also the nature of the event and context itself (Clark-Polner et al., 2016). For instance, studies have found that ANS indicators that are concurrently happening with fear reports are strongly tied to specific context and situations (Mendes, 2016). In an IS setting, it means that neural activities should be tied to the *typology* of not just the "fear" in fear appeal, but of the fear appeal as the whole integrated into the wholistic risk avoidance experience. In other words, every instance of fear is embedded into the sum pattern of neural activations in coordination under particular context. We may as well be able to observe stable activations of specific physiological responses cooccurred with a certain feeling of fear, but only under *consistent* contexts and empirical similarities. It is the consistency of the context that ensures stable patterns of observed experience, behavior and neural patterns, not the consistent meaning of the linguistic label of emotion the similar patterns in physiological activation. Unfortunately, many studies that claimed hard evidence of neural patterns for different emotion categories only mistakenly interpreted the patterns as evidence of meaningful brain states for specific labels

of emotion rather than as encapsulating statistical summaries for the event itself (Siegel et al., 2018). Fear, in short, is not a concrete and stable construct exhibited in different mental states, but part of the observed variances in different mental states themselves.

Although this view of emotion seems to be diminishing the tendency for neural-science-positivism (Medin & Ortony, 1989), we see it as effectively bringing more opportunities for IS research. Although Warkentin et al. (2016) did not observe the activation of amygdala, they did find activations in areas which the authors did not regard as relevant to fear or any emotion. It could be that the specific fear for that context was correlated with those representations. However, if we have the belief that neural activations in the brain have one-to-one correlations with the same construct across contexts, we might not come across such urge to explore in future research. While IS has been striving for its unique positioning among other social sciences with longer history and more theory development, our field could may been already unique from the neuroscience point of view. The critical task is not to "rigorously" establish benchmarks of fear based on previously summarized patterns in psychology, but to discover from scratch, the relationship between security threats and statistically significant neural patterns or other behavioral marks in IS contexts. With consistent context and study design, variations in physiological aspects may be observable and stable enough to correlate with experienced fear, thus being able to predict the relationship between fear and different dependent variables of interest, in a contextually limited but practically relevant fashion.

Readers may have noticed that although we directed the "truth" away from a static and localized view of fear measurements, we have been implying that the "golden standard" of fear is the subjective feeling of fear, or subjectively experienced fear. Next, we turn to its justification and what it implies when experienced fear is not to be the standard from which to derive the justifications for other measurements. From there, we further discuss when external (if neural activations can be seen as external to the individual's subjective experience) measurements may not ever be an "objective" measurement more "accurate than the user herself", and when it may be more suitable than self-report or self-experience, if we still label such situations as "fear-relevant".

3.4 On the Making of Fear

3.4.1 Defining and Implementing Fear

There are two different directions in defining emotions as described by LeDoux (2008). One approaches emotion in a top-down way, seeing human introspection and the linguistic labels (e.g., fear) we attribute to our experiences as the priority (LeDoux, 2008, p. 70). In this situation, the neural correlates which can be argued to encapsulate fear have to present in parallel with self-reported fear as a derivative basis. It is essentially the feeling of fear that delimits what can be

regarded as the neural correlates of fear. Alternatively, one could approach fear in a bottom-up way, seeing fear first as identifiable organism responses when facing danger (also see LeDoux, 2008, p. 70 for more descriptions). This priority emphasizes functional patterns in externally observable behavior and neurology. But it also excludes subjective feelings in many cases, which is prominent for animal studies (Olucha-Bordonau et al., 2015; Suvak & Barrett, 2011, p. 5) since they cannot directly communicate with human. In this situation, if a behavioral pattern is observed and defined as fear in the first place (as it shows the avoidance of danger), researchers may further identify stable neural activation patterns that accompanies this adaptive behavior, effectively nominating summarized neural pattern as the legitimate representation of neural fear (see Suvak & Barrett, 2011, p. 5 for more examples). Still, in practice, we can also view neural responses per se as fear in the first place, although by calling neural response a *response*, we already imply that it is responding to certain perceivable stimuli in the outer world. If no aversive behavior observed, or the study subject does not actively report fear, labeling any neural activation as fear may only represent how the brain response to the stimuli per se. The "fear" is already a different semantic symbol not in common with what we label as fear in daily language.

The specific priority or direction in defining and implementing fear measurement may not imply absolute standard of correctness, but a preference should be clearly realized depending on the research purpose and context at hand. For example, in Hekkala and Stein (2016), emotion was defined as what is shown to others in a collaborative IS project rather than what is actually felt, since the focus of research was the communicative role of emotions as a selected display of feelings in face-to-face social interactions. One may hardly imagine that the fear observed here as comparable to the measurement of fear in IS security studies in survey-based self-reports (e.g., Boss et al., 2015). In similar ways, if a study focuses on the effect of written security communication campaign and consciously experienced fear as a predictor for future protective behavior, then measuring self-reported fear may make more sense. If, however, a study uses field experiment which aims to measure uninterrupted security-related behavioral flow, then observable behavioral indicators which does not require self-reports may be more suitable as the indicator of fear. Notice that the initial directions and details in defining, observing and measuring fear already imply differences in the quality of fear specific to the study, and these instances are not really be comparable with each other with the plain linguistic label "fear".

How we define fear, in turn, also affects that how study results can or should be interpreted. Research could produce different versions of experienced fear while designs of fear appeals elicit dissimilar psychological tendencies and contextual responses (see McDermott & Sharma, 2017 for more support). Specifically, the order in which the survey unfolds can limit the propensity of possible mental response in the first place (Dillard, 1994; Johnson & Tversky, 1983; Leventhal, 1970, p. 158). For example, using common rating scale for two different variables may lead participants to implicitly link them together, hence artificially inflating the association between the two variables (McDermott & Sharma, 2017; Podsakoff et al., 2013). Thus, if a survey bundles together questions

on threat severity and fear experience, we could already be nudging participants into conscious reflection of experienced fear as well as *base the evaluations of fear and severity out of each other*, therefore inflating their associations. But in other natural settings, people may simply evaluate fear based on concerns other than severity. On the other hand, if we avoid subjective arbitrariness in measuring emotion and instead viewing physically observable behavioral patterns as fear, then we may have to establish stable (as for the researcher and observer) assumptions on the relationship between the physical, and the experiential or behavioral. For example, we may assume the same observable behavior always represents the same internal organism coordination or risk avoidance rationale. We may also automatically assume that certain stimuli people behaviorally avoid is survival-threatening and consider these behaviors adaptive in nature. Among all these, we should notice that the starting direction has already paved the way for a range of specific possibilities in end interpretation, where there will always be some subjectivity in concrete physical observation (e.g., researchers' subjective defining of survival-threatening to be survival-threatening). Eventually, the subjective is the foundation of claimed objective.

3.4.2 Towards Contextual Rigor

While we have portrayed multiple possibilities in the researcher's active defining and redefining fear, the critical consideration remains to be whether specific arrangements of a study design "match" the typical way people are in contact with specific security threats in practice. One could approach this from ecological comparisons between implemented emotional measurement and how the emotion naturally occurs in practice. In psychology, while one may strive to conduct *rigorous* research that implements comprehensive measurements of constructs pre-defined in risk avoidance theories, it has been found that studies which aim for *dogmatic rigor* rather than creative flexibility are much more likely to fail at replicating appropriate affective experiences, for they tend to measure feelings multiple times (e.g., manipulation check) throughout the session (Clore & Schiller, 2016), which may break the natural flow of emotion in the context (see Nabi & Nabi, 2014 for more on emotion flow).

Do we look away for incoming cars while crossing the road because we feel the fear, we rationally think we should, or we act automatically out of habit? Do we consciously feel fear if we are not asked to rate our level of fear towards the street? Different ways in defining fear and implementing measurement may yield very different answers. The interpretations of them should be combined with the realization and reflection of research decisions being made. To reconcile inconsistent results of fear from IS fear studies, a comparison of the contextual implementation of fear is necessary despite a same linguistic label. Recall that in Warkentin et al. (2016), participants were presented with short *statements* about information security while exposed to fMRI scans at the same time. While this is a typical and a well-executed neuroIS study, we may realize that fear is often not a psychological state that emerges independent of cognitive appraisal (Harris et al., 2016). Just as protection motivation theory suggested (Mewborn & Rogers,

1979; Rogers, 1975, 1983), fear is generated at least in part by what is regarded as the rational appraisals of threat, although we may conceptually label it as a non-rational variable by research design. Note that the statements shown to participants, such as "your computer is in danger of being stolen", are non-inquiries with little context cues, compared to questions which directly asks how much fear participants are experiencing in particular security threat scenarios (Boss et al., 2015). It would be reasonable to see a possibility in which one intentionally initiates mental evaluation of a "fear A" while asked about the level of experienced fear, which is different from the "fear B" peripherally experienced when no such question is present, which could be, again, different from the fear involved in immediate fight-or-flight response whenever it happens. They may each involve distinctive neural activation patterns, behavioral tendencies and experienced qualities.

If we relate this to the examples in Section 3.3.4, we could further see that fear is not a clear-cut entity with one justified method of implementation. It is quite common for studies to discuss the topic of fear while the same linguistic use of "fear" masks *much more critical* underlying implications. For example, while Faizi and Rahman (2020) followed Moody et al.'s (2018) unified model of information security policy compliance (UMISPC) to study the relationship between "fear" and "intention to comply", their implementation of fear represents a different priority in definition. For Moody et al., fear is a subjectively experienced emotion with valence and arousal (p. 289) and their actual measurements highlighted a sense of subjective feeling (e.g., I am afraid of what may happen …). However, Faizi and Rahman's version of fear was more of straightforward appraisals or expected knowledge of threat situations, as the measurements were composed of questions such as "my computer might become slower if I did what Smith did" without directly asking about subjective feelings. We do not suggest either one of them is problematic, but it becomes a problem if researchers intentionally compare their results of the "fear-intention relationship" without intentionally checking if any of the constructs are consistent with each other in different studies. Only when we view the "designed" details of fear, inconsistent quantitative results on the fear-intention relationship between those two studies, if any, might be reconciled. Thus, intentional analysis of qualitative variations of fear could contribute to practical insights beyond the simple discussion of "using fear vs. not using fear" or "how much fear to use to not backfire". Even if researchers should always measure fear in ISec communication research as Boss et al. (2015) suggested, the extent to which measured fears are comparable to each other can vary a lot across contexts. Even as Brinton Anderson et al. (2016, p. 366) suggested, that certain objective measurement of fear (e.g., neural activations) could identify fear even when *the user himself* is not aware, we argue that the "fear" here is in no way the same as consciously experienced fear for the *user himself*, as the active defining of "fear" in such context is already implemented differently as groups of non-experiential neutral activations when exposed to stimulus that are assumed to be threatening, which is not necessarily in correlation with reported subjective experience or practical action behavior.

To conclude, we argue that inconsistent results on fear from neuroIS, survey studies and behavioral experiments already imply different versions of fear to begin with. The priorities in defining, operationalizing, measuring and promoting fear may not imply absolute right and wrong, while the critical benchmark is to consider the resemblance and significance of implementing one direction of fear construction versus another. In sum, we actively implement/design/make fear in two ways. First, the first priority in defining fear is set with the context and research need, from where we build other definitions and *proxies* of fear. Second, the type of fear measured from participants is always affected by the arrangements of the study design itself. We can, as researchers, contemplate on the structural differences between implemented fear and how the fear of interest is naturally experienced, in order to gain more ecological viability and enable *consistent* comparisons between studies of similar topics. Next, we further elaborate the importance of this consistency and how the analysis of consistency may serve as a benchmark itself rather than any single version of fear.

3.5 Practical Implication: Consistency as the Benchmark

To resolve the multiplicity of fear's potential differences over contexts, we propose the critical importance of *consistency* in research and practice. For the measurement of fear, we should not see old benchmarks of fear in dissimilar contexts from psychology as the only proxy of fear. Instead, we can explore unique connections of neural correlations, behavioral patterns and experienced fear in consistency under specific IS security contexts. Comparable results from fear research come from the consistency of context, not from the shared linguistic label of "fear". There are tremendous possibilities in expanding current research schemes and exploring an updated view of fear for ISec communication. We discuss such opportunities and provide a hypothesized case later.

3.5.1 Opportunities in the Pursuit of Consistency

To maintain the consistency between measured and implemented fear is to grant a clear view between fear as physiological activations, fear as adaptive behavioral tendency and fear as direct experience. IS research may first make conscious decisions in realizing the priority in defining fear and how this directs (even dictates) the end interpretation of fear in specific ways. New benchmarks related to different taxonomies of IS security scenarios (e.g., Padayachee, 2012) could be studied as the basis for IS research. Variations in physiological activations and their phenomenological correlations may be explored, instead of viewing them as irrelevant noises. For example, a two-stage fear response was distinguished in a health psychology study that involved recorded video and voice as persuasive material (Ordoñana et al., 2009). The first stage response involved increased attention and orienting marked by increase in skin conductance and decrease in heart rate. The second stage response involved possible classic flight-or-fight

tendency when subject feels imminent danger, which was marked by increased heart rate. Note that even though the activation pattern of heart rate goes in opposite directions in the two stages, they are unified in one holistic fear experience with the specific health-promoting fear appeal implemented in the study. By combining different physiological markers with qualitative behavioral reports in finer granular, it was proposed that the second stage associated more with actual intention to cope, and the first stage more with only attitude changes.

One may identify differences in similar behavioral intervention process from a multitude of aspects related to the taxonomy of communication, such as mode of delivery, contact time, duration, adherence to delivery protocols, etc. (Abraham & Michie, 2008; Davidson et al., 2003). To give a potentially example, we could begin by simply observing the most identifiable variables in particular information security contexts and hypothesize their relationships with different versions of fears. Some security coping contemplation requires psychological propensity in detection, such as performing schedule-based active virus scans. Other security copings may involve more in prevention, such as not open email attachments from unknown senders. The former involves active planning and attention, which is a kind of *approaching*. The latter though, involves a kind of *avoidance*. The neural correlation of these two scenarios, while both could be simply summarized as related to fear, may exhibit the difference in these two kinds of somewhat different mental states, that of approach vs. avoidance which come in bundle with the whole fear experience.

Above all, we believe the power of identifying contextual consistency between different instances of fear research, as well as general affective research, which may be further applicable to IS research involving subjective psychological constructs in general. The fear in fear appeal may not be instantiated as the same abstract construct across contexts, but as multi-dimensional measurements that vary in both the physiological and the phenomenological domain, with actual research scope and reality constraints. In the following section, we provide a hypothesized case analysis to illustrate the potential multitude of fear and one way to identify its consistency in that context.

3.5.2 A Case Analysis on the Consistency of Fear

Our hypothesized case is a scenario where the user experiences fear towards ISec-related threats. The analysis will render a specific "fear" in relation to a multiple of factors worth exploring. The scenario itself can be simply described as follows. Imagine a user uses her personal computer for work. A warning window accompanied with a sound effect suddenly interrupts her work and displays information about a potential ISec threat which needs to be handled by either clicking on "ignore" or "proceed".

We first plainly describe the hypothesized phenomenon. We may see the warning window happen in a sudden, which visually covers her work-related interface, aurally cooccurred with warning sound, and textually display information about the threat itself, waiting to be responded by the user clicking on one of the options. We also see that this might be a short event which requires

compulsory user attention. In real cases, maybe other windows would be greyed out and the system will be usable again only if the user handles this warning first. All above may contribute to a certain fear the user is feeling. The brain activation, if measured at this point, may correlate with a synthesized multitude of the whole experience. We do not know if the user would consciously use or use the word "fear" solely to describe her experience, but researchers may use this word to specify part of the experience, such as certain physiological activation or the totality of the affectionate part of actively self-reported experience. The following analysis represents only one possible way to dissect the fear involved, as we emphasize the assumed suddenness and multimedia presentation in computer interface.

There is often a sense of "being at the moment" when we experience or express emotions in action (Clore et al., 2018; Clore & Schiller, 2016), as emotion confers value on whatever is attributed in mind at the time (Casper, 2001; Clore et al., 2018; Clore & Schiller, 2016). This temporary nature may explain the discrepancy between its effect on attitude and behavior, as fear was once found to be much more positively correlated with attitude than with behavior since from early health psychology research (Leventhal, 1971; Rogers & Mewborn, 1976). During a momentary episode, emotions often have *intentional objects* towards which people have affective feelings about (Casper, 2001; Clore & Schiller, 2016). This is to say that people do not only fear. They can fear a fear appeal as a whole, a specific outcome of the threat, or even the way the appeal is presented, depending on what the temporal attentional focus is. Fear that is being felt can be attributed to the expected object of judgment in order to result in expected influence (Casper, 2001, p. 41). But quite often, the object that is most easily attributed is the most salient one instead of the most important among all the attributable in the environment. For example, what scares people into coping may be a sudden sound and visual interruption of a warning dialogue on a computer, rather than the content of the written text. Moreover, even when the initial attribution is set at one moment, misattribution (Rohr et al., 2015) may happen in the next. For example, when being angry at some sudden news in life, one may be angry at something irrelevant to this original news in the next moment, simply because she happens to be dealing with it in the middle of the emotional episode. Therefore, it is sometimes hard to distinguish one's pre-existing emotions emitted from the previous moment with one's response to the target at hand in the next (Schwarz, 2000).

Consequently, from a decision-making perspective, one does not always *fear* the "right" object, nor would one always *show fear* for the "true" object. In our scenario, the user may be startled by the unexpected change of user interface, the sound and color of the dialogue window, or hopefully, relevant informational content describing the security threat itself. Any of these can be the object of the fear at the moment depending on the security communication design and user experience. Since the possibility of emotional misattribution, the final decision to be made could be in more or less consistency with the initial cause of fear. Two inconsistent scenarios may happen. First, if the user is only startled by the sound effect and other presentation format of the window, she may engage in avoidance

of the presentation window itself, by quickly clicking on an option, even if the button offers a more secure solution. In this case, it may be hard to expect similar risk avoidance behavior happening again when similar fear appeal is embedded in *other forms*. The second inconsistent scenario occurs when the user pays attention to written warning content, but her fear for it may be misattributed to the presentation format. The user may still behave in a way the coping recommendation suggests, but again, it may be difficult to guarantee that the same fear appeal works in other formats other times.

We can see that the user does engage in recommended risk avoidance behaviors out of fear in both scenarios, but the object attached to the alleged fears varies. Early research has showed that only fear which has a clear object may increase persuasive effectiveness, but neurotic fear (i.e., a general sense of fear with no clear object attached) tends to decrease persuasive effectiveness (Leventhal, 1970, p. 138). Is it just enough to make people feel fear? Are we trying to make people fear a certain aspect within the fear appeal environment? If the final goal is not to scare people into one-time security coping, but to promote a certain connection between security threats and coping responses, we may need to rethink what would be the most stable and most identifiable object of fear, that could stay *worth fearing for* over the long run. The insights from this simple scenario, expandable and questioning how we may keep consistency in the implementation of future instances of similar fear in research and practice. For example, for the emotion fear to be a stable predictor of coping behavior, we may want to ensure the object of fear to stay consistent, such that when future evaluation of a similar situation occurs, the fear to be elicited could address the most relevant aspect of the threat rather than rendered invalid. Alternatively, we may also consider how the implemented object of fear can match a natural setting. For instance, it may be alright to focus on the disturbing sound of fear appeal as the appropriate object of ear, as long as most instances that involve the same threat in real life come with certain disturbing aural stimuli. Following this line of thought, eventually, we may decide that the warning design aims at raising current and future perceptual salience of threat through the consistency of implemented fear.

3.6 Future Direction: Emotion into Cognition

Numerous questions could be asked in emotion related IS study. Should we see a momentary fear and a more lasting fear as the same construct stretched in different time span, or should we see them as qualitatively different such as termed by fear as emotion and fear as mood (Beedie et al., 2005)? Do we see fear for virtual stalking and fear for physical stalking as the same fear for different events, or different fears characterized by different feelings, thoughts, attitudes and physical arousals? While stress, cognition, emotion and motivation can trigger the same physiological response (Mendes, 2016), psychology has been using the compound term "affect" to refer to evaluations including affective

feelings, thoughts, expressions, emotions and dispositions (Clore & Schiller, 2016), indicating the intertwined relationship between emotions and mental activities commonly distinguished as rational or non-rational. Our analysis views experienced fear as in a multitude of relations with neural correlates, behavioral adaption, cognition, duration, object attachment, etc., such that it would be unfit to place fear as a single-meaning variable side by side besides what one may regard as the rational cognitive decision-making process.

We argue that the future step in understanding emotions for IS and ISec decision-making entails seeing emotions an integration of episodic experiences characterized by multiple cognitive factors. IS research (e.g., fear appeal ISec communication, affective computing) can benefit from it, as it is in those integrations one realizes the contextual consistency which could be utilized to not only define and implement emotions in IS research, but better understand inconsistent study results across contexts. While the distinction of problem-focused coping and emotion-focused coping (Liang et al., 2019; Liang & Xue, 2009) could explain ISec phenomenon, it is only one way of summarizing coping modes based on their observed function (Lazarus & Folkman, 1984, pp. 148–150) in the individual's altering of person-environment relationship (Folkman & Lazarus, 1980, p. 223). However, this terminology difference may promote a conceptual separation between rational process (as tied to problem-focused coping) and irrational process (as tied to emotion-focused coping) in forming protective motivation and behaviors. For example, Liang and Xue (2009, p. 78) hypothesized and wrote, "to the degree that IT users are rational, they will try problem-focused coping first". To further understand emotion and reconcile IS studies beyond the discussion of "fear vs. ration", we encourage researchers to view emotion and cognitive appraisal beyond such dualistic distinction, not as different variables elicited by risk and threat, but a coherent process with rational conflicts (Helm, 2010).

One immediate benefit is the justification for consistent ISec communication results without the focus on a naïve concern of a "fear issue" that discusses its role of backfire or not. To integrate fear with evaluative appraisals, we may classify appraisals of threatening scenarios into finer categories in relation to various adaptive affective tendencies, such as appraisals of pleasantness, anticipated effort, attentional activity, certainty, responsibility, control, legitimacy, and perceived obstacle (Smith & Ellsworth, 1985). Previous studies suggested that different self-reported emotions often co-occur with different subsets of cognitive appraisals (Ellsworth & Smith, 1988; Oatley et al., 2011; Parkinson, 1997; Smith & Ellsworth, 1985). For example, fear was found to be highly correlated with appraisal of uncertainty, perceived obstacles, importance and personal control in some non-IS contexts (Dillard, 1994), in which we could see fear *as* a synthesis of these cognitive appraisals *themselves*. Note that the relationship between emotion and appraisal, just as other categorizations of emotion we addressed, may vary with contexts (Parkinson, 1997; Roseman & Evdokas, 2004; Tiedens & Linton, 2001), and they are not deterministically componential, meaning that no particular appraisal may be necessary or sufficient for a single emotion across all contexts (Kuppens et al., 2003). However,

we may still be able to identify relatively stable appraisal patterns associated with emotions under specific IS contexts. This analysis allows us to view fear and other emotions as channels through which one casts evaluative value for judgement (Helm, 2010, p. 16), but not to regard fear as a separate variable in addition to these evaluative processes. Thus, it allows flexibility in designing fear appeals tailored to contexts and tuned for more similarity between overall affective patterns and the judgments to be made (Clore & Schiller, 2016).

We propose that a dichotomy of emotion and cognition should recede into a secondary position. Instead, researchers may focus on why and how people comply with what kind of fear, under a context with what characteristics that shapes the fear uniquely. To truly deepen the affective process in IS studies, we encourage to view fear and other emotions not in discrete systems in isolation but to hypothesize how a range of facets may act in concert with one another (Campos et al., 1989, p. 395).

3.7 Conclusion of Study 2

Problem

IS research have proposed the possibility of fear as a multifaceted construct, but no study has directly addressed this. While more empirical research in IS security measure fear with self-reported data and observed neural activations, inconsistent results need to be reinterpreted in a comprehensive discussion on how instances of fear differ in definition and measurement to start with across studies.

Solution

Our analysis offers new insights in understanding fear for IS research. We explicated the relationship between physiological fear, experienced fear, and behavioral fear, suggesting that different instantiations of fear already have dissimilar (neural activation) patterns from the beginning. More critically, our discussion of the priority in defining and implementing fear suggests that researchers, while all may use the linguistic label "fear", are indeed studying different phenomenon with varied priority fitted to particular research goals. Furthermore, through a hypothetical scenario, we analyzed how a specific instance of fear may qualitatively vary in context. Finally, we propose to view fear not as a separate variable but as a complex process in relation to other aspects within cognitive experience.

Contribution

There are numerous kinds of risk in life. How could we expect the fears involved are all the same even while we all use the same word fear to label them? Our analysis of fear, partly inspired by recent neuropsychological research and classic emotion research, offers reinterpretations of fear for IS research that no study in the field has attempted to untangle. It reconciles inconsistent results from

empirical findings in IS security research and envision a research future where different versions of fear can be equally, as well as confidently, defined, measured, and implemented. Our study is crucial to understanding fear and future emotion related research design for IS security. It is further meaningful for shaping the academic publication atmosphere in IS, and for designing practical information security interventions.

Recommendations

- Reestablish the benchmarks of neural correlates of fear for IS research instead of simply relying on previous results in psychology.
- Clearly reflect on the priority in defining and implementation of fear and other mental constructs in IS research, whether as a self-reported subjective feeling, observed adaptive behaviors, summarized neural activations, etc. Researchers should consciously notice that such different priorities may or may not be suitable to be compared with the purpose and context of other research and practical settings, and they should aim to address how the way affect is defined influences the possibilities in the final interpretations of study results.
- Explore the consistency between instances of fear implementation in research and practice. Use qualitatively analyzed consistency as the benchmark for comparable and reliable research design.
- View fear as integrated into the cognitive appraisal process rather than always a separate irrational variable that affects intervention results in regression models.

4 STUDY 3: A CHANGE OF MIND: BEHAVIORAL THEORY AND INFORMATION SECURITY COMMUNICATION AS BODIES OF KNOWLEDGE FOR DECISION-MAKING SUPPORT

Information systems (IS) security research have relied on behavioral and communication theories to predict and improve information security (ISec) behaviors. In practice, ISec communications are designed and implemented based on such theories in hope of achieving expected persuasive effects. However, as persuasive results fail or fade over time, a more fundamental discourse should describe and discuss how people engage in the simple, daily, common, yet "unpredictable" act of having a change of mind after their initial decision-making result.

In this section, we propose a new framework for understanding behavioral theories and their communicative application in ISec management. We start by introducing two complementary assumptions and their implications. First, we assume a fully rational human's behaviors as inherently unpredictable, and the level of unpredictability increases as the individual incorporates more diversified sources of information to support their flexible decision-making process. Second, we view theory and its communicative application as temporary bodies of knowledge that recipients more or less utilize for making decision. With such problematization, we discuss the validity and effectiveness of behavioral ISec theory and communication implementation in both shorter and longer terms, which conceptually addresses the importance of the flexible use of behavioral theory, as well as practically informs varied strategies based on communication's capability in promoting recipients' extended information gathering at the time of persuasive delivery.

Overall, our analysis offers a new framework for understanding behavioral theories and discuss practical implementation strategies towards sustainable ISec communication results.

4.1 Introduction to Study 3

User behavior plays a critical role in information security besides sheer technological implementation (Sasse et al., 2001), and information security would be evermore relevant to people in the ubiquitous computing environment in becoming (Hayat et al., 2007). Thus, a key endeavor in information security (ISec) management is to *communicate* information about security threats and recommended behavior to users so that improved behavioral compliance could be achieved (e.g., Johnston et al., 2015, 2019). Here, we use the term *ISec communication* to refer to a set of different persuasive means that attempt to communicate persuasive information to people (e.g., employees and citizens) in hope of changing their attitude, intention, and behaviors towards improved security practice. This may include purposefully distributed content in various forms, such as persuasive message (e.g., Johnston et al., 2019), system warning (e.g., Vance et al., 2018), organizational policy (e.g., Siponen et al., 2014), awareness training (e.g., Shaw et al., 2009), etc. For our scope of discussion, we view such ISec communications as various forms of information or knowledge delivery.

In IS research, communicative means are often based on behavior theories which often model how people perceive and cope with threats. For example, many persuasive messages (e.g., Boss et al., 2015; Haag et al., 2021) for ISec management were designed based on protection motivation theory (PMT, Rogers, 1983), which argues that people rationally evaluate risk based on a finite set of factors, such as threat severity, personal vulnerability, self-efficacy, and coping efficacy. Correspondingly, a persuasive message based on PMT could be compartmentalized into semantic components each contains information or knowledge on one of these theoretical constructs (Johnston & Warkentin, 2010). In our discussion, such communicative messages are viewed as specific arrangements of knowledge that carries persuasive power, if believed.

In practice, the knowledge belief with which the individual makes decision could vary or mutate, as people's reason of behaving in certain ways change in different contexts (Karjalainen et al., 2019, 2020). We argue that the lack of the conceptual discussion of such changing nature of human behavior and decision-making knowledge support undermines our flexible use of behavioral theory and strategic design of communication, potentially leading researchers to abide to established constrains and guidelines (Boss et al., 2015; Gregor, 2006; Lee et al., 2021) that could hinder research progress. Achieving long-term persuasive results may entail the combined use of multiple theories with different underlying assumptions, as well as communicative interventions capable of considering the people's undergoing life events and their circumstantial characteristics (Hsee & Hastie, 2006). Our discussion, in turn, offers the conceptual foundation to understand and justify such flexible use of theory and rationale for communicative strategies.

This study has two objectives which converge into one core conclusion. For one, we portray the level of human decision-making predictability (i.e., flexibly generating preferred behavioral choice based on available information synthesis) by introducing a behavioral-economical model where a *fully* rational human's preferred behavior in a somewhat complicated scenario is regarded as inherently unpredictable (Heiner, 1983, 1985, 1989). By this, we describe how the gap between the human agent's competence (i.e., C) in gathering information for decision-making and the difficulty of decision-making scenario (i.e., D), together (i.e., C-D gap), characterize the predictability of decision-making results (e.g., intention and behavior). For the other objective, we support the flexible use of behavioral theory that addresses such variations in behavioral predictability, by viewing theories and their communication application as the production of temporary knowledge with power (e.g., persuasive influence) implications (Foucault, 2007; Foucault et al., 2008; Foucault & Gordon, 1980).

Combining those two assumptions, we discuss the stability or the predictability of ISec communication results in relation to time and information diversity offered by the theory-based communication itself and after-delivery environment. Overall, we view behavioral theory as summarized behavioral rules, its communicative application as knowledge-power relations for individual's decision-making support, and the communicative results not as immediate intention and behavioral compliance, but established knowledge beliefs and their chance of serving as stable information source for supporting decision-making. We offer a framework to understand the short-term and long-term resilience of ISec communication, as well as a justification for the flexible modification and use of behavioral theory in IS.

4.2 Why ISec Communication Results Hardly Last

In this section, we portray the fundamental rationale that ISec communication results do not last in the long term. For one, we portray the predictability and unpredictability of a rational human agent (Section 2.1) based on Heiner's behavior-economical model (Heiner, 1983, 1985, 1989). For the other, (Section 2.2), we view behavioral theories and their application in communication as the identification and the production of temporary knowledge-power relations (Foucault, 2007; Foucault et al., 2008; Foucault & Gordon, 1980). Together, they form the conceptual ground for describing the mutation of ISec communication results (Section 2.3).

4.2.1 Fully Rational Human Behavior as Unpredictable

Commonly used theories for ISec communication research portrays how a human agent engages in predictable risk evaluation patterns in fully systematic or rational conditions. To name a few, protection motivation theory (PMT, Rogers, 1975, 1983), theory of reasoned action (Ajzen & Fishbein, 1980), and deterrence

theory (Gibbs, 1975). However, in practice, individual's reason, or the evaluation patterns, for compliance or noncompliance of security recommendations may change over time (Karjalainen et al., 2019; Siponen et al., 2018). In other words, if they are rational, their way of being rational changes over time and context. Thus, the framework for theorizing the long-term change, or further, the general stability of ISec communication results, has to account for the unexpected side of human behavioral patterns.

We introduce Heiner's model of rational human behavior (1983, 1985, 1989) to account for unexpected decision adjustments people could make even after they initially commit to one certain "best" choice for a given problem. In general, the model proposes that the *more* rational the human decision makers are, the *less* predictable their decision-making results are (i.e., statistically how accurate an observer can predict an individual's preferred behavioral choice for a given problem). A key concept that portrays such change of predictability/unpredictability concerns the *gap* between an agent's *competence* (e.g., perceptual ability in deciphering the relationship between behavior and environment, denoted as "p") and the *difficulty* of the decision problem (e.g., complexity of environmental situations related to the decision-making, denoted as "e"), which is termed as the *C-D gap*. The model suggests that it is not the absence of C-D gap, but rather its presence which conditions regularity in behavior (Heiner, 1983, p. 563). In practical terms, as the decision maker gathers more information sources (e.g., opposing viewpoints that the observer has not thought of) and take them into account, the more unpredictable their decision-making results (e.g., intention and behavior) would be (holding others constant).

Following this thinking, observed predictable behavior patterns at one moment can only be understood as *behavioral rules* that arise because of the individual's uncertainty or inability in realizing better coping behaviors (Heiner, 1983, p. 561). When uncertainty is present, the rational decision maker, due to the lack of information sources to support flexible decision-making, is more likely to restrict her flexibility and stick to limited information as decision-making support (e.g., information a communication message provides), thus producing simpler and more predictable behaviors. However, when the decision maker's competence increases, she is able to take more environmental factors into account, which generates increased decision flexibility, producing more unpredictable patterns (from the observer's perspective). For example, in Albrechtsen and Hovden's (2009) study, the observed difference between security managers and employee users in practicing ISec behaviors was framed in relation to the user's limited security capabilities and motivation (Fig.4, p. 488). In our line of thinking, it can be viewed as the user's increased capability of flexibly making decisions based on richer contextual information in their actual life. For instance, it could be the users' improved clear realizing of work and life priorities that are more important to themselves which result in less security compliance. While readers may argue that this viewpoint is only a human-centered change of *language use* to describe noncompliance behaviors, we argue later that this change of view provides strategic and design implication in applying behavioral theory and ISec communication.

Next, we summarize the assumption and relate them to the understanding of behavioral theories for ISec communication. First, a rational person is capable of making informed decision by synthesizing information from multiple sources, not just a limited preset of information sources. Second, the more able one is in gathering information to support decision-making, the less predictable her behavior could be, characterized by the shortening of C-D gap. Lastly, implied by the relationship between C-D gap and level of predictability, predictable behaviors are more likely to be observed when the decision-making scenario stays similar, where the decision maker is only able to gain limited information that the observer also shares knowledge of. Overall, the predictability of behavior varies with the contextual complexity of decision-making scenario and human's capability of incorporating rich information sources for such decision-making needs.

Consequently, a couple of preliminary proposals could be drawn with regard to the use of theory for communicative implementation. First, any single behavioral theory, such as PMT, may not *ever* be the best theory to model ISec behavior in the long-term, since the contextual change over a longer period of time renders the decision maker's information source diversified and her capability of making use of information varied. For example, PMT was designed to explain people's deliberate and systematic cognitive evaluations to fear appeals (Maddux & Rogers, 1983, p. 470; Rogers & Steven, 1997, p. 114). But the fear appeal stimuli do not persistently present after initial exposure, and other information sources may become more relevant for decision-making support, such as perceived social norms and the shift of work priority. In this sense, if we use PMT to predict long-term behavior, we may benefit from combining it with another behavioral theory that accounts for the effects of social norm, given that we expect such factors would be present and relevant in the decision-maker's long-term decision-making support. Thus, the original PMT, in this case, may be a better theory to predict and explain behavior when the decision-making scenario is limited to only short-term presentation of fear appeal under time pressure, where people do not have access to other information to support decision-making. A modified PMT, perhaps, would be more appropriate to model long-term behavioral change.

Second, while behavioral preferences may be unpredictable in a longer time span where more information sources can be incorporated by the individual to support decision-making, it *may* be possible to predict *the degree of unpredictability* statistically by the expected change of information complexity relevant to decision-making (Heiner, 1985). If we have to predict the future from a distance, a certain "meta-model" is required which accounts for the probabilities of different decision contexts' occurrence over time and their inter-similarities with each other, as well as the probability of a human agent's commitment to a certain "preset" decision making process and results (e.g., as portrayed in PMT) under different types of contexts (Gilboa & Schmeidler, 1995). For example, we may expect that a user complies to secure behavior in the company scenario *stably* to avoid punishment (e.g., explained by antecedents described in deterrence theory). We may, meanwhile, expect the user stably *not* complies to the same secure

behavior at home based on avoiding extra cost this behavior takes. If the user's commitment to secure behavior is respectively stable in those two contexts, and the two contexts' relative occurrence in the user's life also remain stable, then a way to predict her overall commitment to compliance is to consider the frequency of the two contexts' ratio in her life and her respective commitment to compliance in them, so that an integrated version of communication may be designed that targets such divide of behavioral pattern in company and home. Correspondently, the model capable of explaining her overall commitment to compliance could be a weighed combination of deterrence theory and a contextual factor of perceived behavioral cost.

4.2.2 Theory and Communication as Production of Bodies of Knowledge/Information

In the previous assumption, we view behavioral choice as the outcome of the agent's rational synthesis of information for decision-making support, among which the content of ISec communications is a main type that a typical ISec behavioral study may pay attention to, such as written policies, fear appeals and other general persuasive messages, where selective information about the threats, context, technology, etc., is presented. For instance, the written punishment for privilege misuse in a company document can be regarded as informational knowledge on the link between actions and reprimands. However, such information is not a "pure" form of knowledge with no real-world consequence. They are the basis for people's actual decision making, which result in unobservable psychological influence as well as observable behavioral outcome. In other words, they bear the *power* (e.g., direct persuasive influence) of affecting intentions and behaviors which bring further consequences.

We have argued that a behavioral theory is only a summarized set of "behavioral rules" that individuals are observed to tend to follow in particular situations, before they could synthesize more information to support a different decision-making process (which yields unpredicted results once it happens, compared to a previously observed regularity in behavior). Combined with the viewpoint of information as knowledge that carries power implications, we introduce the second assumption, where behavioral theories and its communicative application are only specific arrangements of power-knowledge relations and their managerial production (Foucault & Gordon, 1980; Willcocks, 2004, p. 254). This assumption is two-fold, in that the theory is regarded as a summarized behavioral pattern observed for an individual when she is unable to utilize more information for decision-making in particular settings. Also, a theory's communicative application (e.g., a persuasive message based on a behavioral theory) is viewed as produced informational knowledge based on such speculated behavioral pattern, but with potential power implications for decision-making support. Note that the "power" here does not necessarily imply negative implications as perhaps in the term "totalitarian power". Rather, it refers to the general implementation and deployment of a relationship of force

(Foucault et al., 2003, p. 15) that both the communication issuer and the recipient may exert onto each other.

For example, a fear appeal message is nothing more than a set of *provided* knowledge about a threat's severity, agent's vulnerability of being exposed to the threat, recommended coping methods to mitigate the threat, etc. It is the temporary acceptance of this knowledge that the support the individual's decision-making results in a way predictable right after the intervention. However, as the rational decision maker gathers more relevant information to support her active decision-making, her behavior become more unpredictable compared to the previously observed compliance right after appeal delivery. In this sense, the knowledge from the initial fear appeal communication turns out to be only *partial knowledge* we wish the recipient to consider during message delivery. In a longer term, more knowledge and information (e.g., the decision maker's belief that she is not really that vulnerable to such threat) is generated and incorporated as decision-making support, which contributes to updated decision-making and yields unpredicted behavioral results (compared to the initial results). It is in this sense, that the *strategy* for theorizing and implementing solutions for behavioral change should account for the required temporal validity (e.g., how long we need a persuasive result to last) of persuasive results and the individual's future capability in integrating different knowledge for making decisions.

Readers may wonder why we describe fear appeal's fading effect via such a perspective change that could simply be put in daily language as "people's reason of behaving change". This is because, such transformation of perspective, although only to describe the straightforward phenomenon that "people's reason of doing things *can* change", bears implication on the flexible use of theory and strategic deployment of communication in ISec research. If we strictly follow guidelines such as Boss et al.'s (2015) recommendation of admitting the core nomology of PMT as the correct version of this theory, and measure theory effectiveness based on the metric of model fit, we may implicitly attempt to look for a "best" theory for given behavioral ISec problems where the same set of identified cognitive factors result high effectiveness in both short and long period of time. If we accept Lee et al.'s (2021) proposal of self-evident axiomatic theories, we may set a goal of constructing such a theory for behavioral ISec or simply regard an established behavioral theory in the field as an axiomatic theory. However, if our assumption hold, such research practice or inclination will not be relevant, as the theory choice and communication design for maximum short-term results and maximum long-term results, even for the same security behavior in the same context, does not need to be the same.

Others may wonder why we do not simply frame our discussion under the notion of "stage theory" to frame our discussion. For that, we emphasize that while stage theory could be considered as one possible way to address unpredicted behavior (e.g., noncompliance occurs at certain stage and what factors may get the individual "back on track") after initial exposure to intervention (e.g., the first stage), it still assumes the change of people's behavioral pattern follows a specific trajectory described in stages, each of which

contains a set of factors contribute to a persuasive effect for a given issue. Our viewpoint in seeing the level of potential unpredictable behavior relative to the change of C-D gap, as well as seeing theory and its communicative application as temporary knowledge production, is arguably more fundamental, and it has a significantly distinguished focus on knowledge stability, which yields research implications among which justifying the use of stage theory is just one.

4.2.3 Why ISec Behaviors Hardly Last

Our assumptions portray why and how ISec communication results may not last long *enough*. Specifically, contextual changes may often offer the individual more varieties of information at potential disposal to be accounted for decision-making (the shortening of C-D gap), where the user more flexibly makes unpredicted decisions (compared to the previous one) regarding the same ISec problem.

This explains certain "deviances" in security compliance, which we frame as the change of knowledge-power relations from the flexible use of information for decision support. For example, individual's changing understanding of work priority (Albrechtsen & Hovden, 2009) and shift of personal interest (Wall & Buche, 2017) could result in actual deviance from previously practiced security behavior. For us, the ground for modeling long-term behavioral management falls on the assessment of the individual's potential in gathering from various information sources for decision-making, which characterizes the stability of a certain established behavioral pattern (e.g., formed during the initial communicative intervention). *The job of theory and its communicative application, as the identification and production of knowledge-power relations, is to produce arrangements of knowledge that support the individual's rational decision-making in a more or less flexible way.*

We have provided the ground for analyzing why and how ISec communicative results may be more or less predictable/unpredictable. However, we may also benefit from considering "why ISec behaviors" in specific. After all, our introduced assumptions may apply to other risk avoidance behaviors as well, such as workspace accident prevention, voluntary vaccination, mental wellness maintenance, etc.

To simply put, we regard behaviors related to digital technology as inherently encapsulating greater unpredictability in the long run. Heidegger's (1977) pioneering analysis of modern technology frames technology's primary feature as a mode of challenging and stand-reserve type of existential "revealing". For one, there is much more hidden mechanism (e.g., a recommendation algorithm that determines what the users could see on a webpage) underlying the direct "revealing" of technology (e.g., what is visually shown on a webpage), hence the "revealing" mode being *challenging* for one to grasp compared to more tangible technical and craftsmanship revealing, such as sculpture and fully mechanical artifacts. For the other, much of technological implementation is not being used concurrently but in "stand-by" mode as reservation for later use or occasional needs (e.g., a user only uses a small part of the full feature list that an application provides), which leaves greater room for diversified use contexts

involving similar types of behavior and risk. Together, the challenging and stand-reserve feature of technology bring more variability in contextual change and power-knowledge opportunities.

As many theories for ISec behavioral modeling and communication come from health psychology, we compare ISec and health phenomenon as an example. First, people may lack direct experience and extended knowledge with regard to technology and ISec risk, but arguably almost everyone has had direct experience with illness and bodily discomfort accompanied. Further, although people may not understand the biological processes bound to diseases, their extended personal-social outcome could often be directly experienced. However, security problem may be experienced in much subtler ways with minimally perceivable manifestation depending on the context, and even omittable social effects for the individual herself who situates in an organizational environment (Johnston et al., 2015). While lots of health risks are expected to result in sensible feelings and social predicaments, ISec risks take in numerous forms and each of them may lead to different outcomes in reality.

Thus, security and risk communication functions could be seen as a modern person's *sensory organ* (Lidskog, 2013), through which users receive otherwise unrevealed knowledge and information about risks and understand stand-reserved features of technology. However, as we argued, the user may also come across many other information sources besides those provided in implemented persuasive communication, and thus regularly updating their self-generating knowledge about ISec threats, which encourage more unpredictable decision-making processes across different contexts and time points. The key to strategically incite better short-term results, and on the other hand, sustained long-term results, simply lie in the consideration of the ISec communication's role as an interface in between such knowledge divide.

4.3 Implications on Unpredicted Communicative Persuasion Results

In this section, we discuss a few examples to understand "unpredicted behaviors", not regarding them as "persuasive effect that backfires", but in relation to the change of C-D gap and the shift of knowledge-power relations. This change of perspective is necessary to redirect the focus in viewing risk avoidance theory and ISec communication, from *implementing a set of "cognitive antecedents" that achieves "behavioral effectiveness"* to *providing a suitable "body of sustainable knowledge" for "decision-making support"*.

4.3.1 Example 1: Accurate Prediction

One may predict that her student friend will check email every day, and such prediction can be very accurate, since the social structure is organized in a way (people may call this common sense) that students need to check emails regularly

for school-related agenda. In our framework, it reflects matching C-D gap and a shared body of knowledge to support decision-making of "checking email every day". For both the one who intends to predict, and the ones being predicted, they share similar existing knowledge beliefs, such that "checking email is necessary for a student's normal life" and "I want to live as a normal student fulfilling arrange my agendas via email". Further, they have comparable capability for this type of decision problem, such that "checking email" is the only solution for maintaining survival that they know of, but not some new technology that may synchronize people's agendas without the use of an email system.

4.3.2 Example 2: Accurate Prediction that Does Not Last (But Does the Temporary Job)

Imagine a customer shopping for a camera at a store. The guide may introduce a large number of useful functions to the consumer, including dual memory card slots, peak focus, pixel shift, film simulations, etc. The consumer, upon receiving all this knowledge about this camera model, willingly includes all these factors into her purchasing decision and buys the camera, truly seeing it as functional, aesthetic and easy to use, all in one. However, after that day, she realizes that she does not need all these functions for her own purpose of use. Over time, she eventually only cares about the camera's aesthetical features and a few simple functions.

In this slightly more complicated case, the shopping guide creates a power-knowledge environment by communicating the information he finds useful for the consumer. Thus, at the moment of communication delivery, the consumer's mental capability and knowledge is limited to what the guide provides and only provides. For the consumer, her C-D gap is limited to a certain point without extended information sources. The assessment of such persuasive effect should be dependent on the perspective. For the guide, his "behavioral theory" about the consumer's buying decision worked, but only for a day. For the guide's own work performance purpose though, it may have been successful. Described in our thinking framework, he applied a specific power-knowledge environment around the consumer and validify of such relation slowly changes after the initial purchase.

Alternatively, we can imagine another consumer who had a chance to try the product first as well as browsed the internet for some third-party camera reviews. She may end up buying a cheaper camera with less features, but the decision may be more stable in the next day and days following, since she already incorporated more information at the time of decision-making, which makes the overall results more "resilient" to out-of-current-context factors she already rationally considered. Although she did not spend as much money or acquire a camera with more features, her long-term satisfaction with the decision improves. In this case, we say that consumer herself co-created the knowledge-power relations by actively and deliberately gathering more information. Or in our terms, she decreased her C-D gap for the decision-making of buying a camera. That, in turn, weakens the guide's persuasive power at the time of

persuasion delivery, which yielded a purchase decision not as entirely as what the guide predicted, but a result more stable in a longer period of time.

4.3.3 Unknown Knowledge for Unpredicted Behaviors

With previous examples, we intend to show that the key to think about long-term predictability is to consider the change of C-D gap with extended or limited gathering of knowledge and information (we used these terms interchangeably although knowledge is arguably one type of information). To extend the chance of knowledge gathering, is to grant the decision-maker "space" for considering any other information and compare them against what is available in the communication. It may result in more unpredicted behavioral rate (compared to what the communicative intervention intends), but the measured initial decision may be more resilient. To limit the chance of knowledge gathering, is to have the individual's attention and scope of thinking fixated at the knowledge presented, hence eliciting expected persuasive power. This, to us, characterizes the flexibility of IS communication in two senses. *First, communication design could shape and present the knowledge in a predesigned way under a well-controlled environment. Second, it may also further motivate the individual to gather extra information on top of what itself provides for decision-making support.*

There could be a significant degree of freedom for the communication to frame or present knowledge in different ways. Risk, as the most basic concept in risk management, refers to a state of affairs in which undesirable events may or may not occur, indicating something unknown or capable of bringing an unknown outcome, for which a human lacks knowledge of (Hansson, 2018). This *knowledge about the lack of knowledge* (Hansson, 1999, 2018) could be framed differently depending on the communicative needs, such as how possible a risk may occur and how vulnerable individuals are. As one may lack knowledge of the outcome, probability, implicit assumptions, and other parameters concerning a particular risk (see Riesch, 2013 for different levels of uncertainty), there is extensive flexibility for ISec communication design to frame a risk as of a certain nature but not others. There could also be many aspects of knowledge that a communication intentionally or not intentionally includes, such as technical difficulty, economical consequence, and indirect social-political implications (Chicken & Posner, 1998, p. 158). The less tangible a risk is, the more degrees of freedom and possibility there may be in producing bodies of knowledge related to it.

Consequently, in risk management, the organization may wish to limit the amount or type of information provided to an audience concerning a risk, in order to achieve specific management goals (Lundgren & McMakin, 2018). Similarly, in IS research, efforts were spent manipulating levels of variables in theory-based communication designs. With "threat severity", for instance, one may frame a risk as "not severe", "severe" or "very severe", which could lead to different levels of persuasive result at the moment, but overall, all human practices involved would shape the formation of knowledge over time (Henriques, 1998, p. 24). In this regard, unpredicted decision-making results

come from the temporary communication's inability to motivate and consider out-of-theory knowledge-power connections.

4.4 Implications on Evaluating Persuasive Effects

We have framed the expansion or limitation of "knowledge", which bears power relations, as the critical measurement for more predictable or unpredictable decision-making results across context and time. In this section, we discussion a possible way to analyze such knowledge-power relation for ISec communication.

In Foucauldian analysis, where we draw the connection between knowledge and its persuasive power implication, the general concept of security is considered within a *tension* between individual interest and interest of all (Foucault et al., 2008, p. 84), the structure of which resembles recent behavioral ISec studies (Karjalainen et al., 2019, 2020) that adapted "dialectical tension" as the basic unit for analyzing dynamic ISec perception and behavioral change. Such perspective is helpful in understanding changes that emerge through the resolution of conflicts between opposing forces (Karjalainen et al., 2019, p. 691). For our discussion, it shifts the focus of evaluating persuasive effectiveness of a communicative intervention from "what behavioral antecedents lead to what results" to "where the power of communicated knowledge is situated in a dynamic tension".

Thinking in tension is different from modeling variables and their static relationships. The same variable, such as "behavioral cost of adapting a secure behavior", may imply different significance when situated at different ends of tensions, such as in the tension of "individual self-control vs. institutional management" (i.e., the basic tension between the individual's desire of self-control and her conforming to collective management). It could be that high cost does not cast a problem when the necessity of collective management is prioritized by the individual. However, it may be a problem when she leans towards the need for self-control in another context that involves the same threat. Although there can be numerous sets of variables that affect security-relevant behavior in different contexts (e.g., as described in different behavioral theories), the framework of tensions may be relatively stable. For example, as long as the individual has a home and a work life, her basic tension of self-control vs. institutional management continues. While many variables could emerge, such as new work goals, behavioral cost, reward, life events, etc., they may either address her need of self-control or the willingness for submitting to institutional management. We may then ask questions such as whether the behavioral cost of complying to certain policy at home can be reduced by technical implementations, or whether rewards can be implemented for her own needs of self-control, besides those for implemented for management requirements.

While Karjalainen (2019) has proposed tensions in employee's ISec behavior such as "trust vs. suspicion" and "individual vs. institutional", we incorporate them and consider new ones for sustainable ISec communication. We approach

the basic tensions in the delivery and maintenance of ISec communication with the rational belief of knowledge as a core, which aligns with our assumptions of communication as knowledge and relevant behavior as a consequence of human rationality. First and foremost, the individual either believes the knowledge of the communication or not. To achieve effectiveness, the body communicative knowledge should be believed to a sufficient level so that predicted evaluation by any communication theory may be expected at least at the moment. Otherwise, communication message could be not believed or believed in a way not as the issuer intended. Second, belief could form, but the knowledge may not apply meaningful forces of power if considered not relevant, such as not relevant for the person at all or for the specific action she takes at a later moment (rational human may not use irrelevant information for decision-making support). Third, the individual may believe the content of the communication and consider it as relevant, but the knowledge-power implication could come from external sources, such as company sanction (Johnston et al., 2015), or internal sources, such as personal vulnerability to a threat (Haag et al., 2021). Finally, the believed knowledge and its power relations do not lock into place at one moment but develops over time varying with contextual complexity and human rational capability. Hence, we denote the tension of time. Note that the "time" here implies the change of context and thus more opportunities for the rational human to synthesize different sources of information against their formed belief of knowledge, while continuously supporting their active decision-making process on the go.

4.5 Implications on the Psychology of Time for Communicative Persuasion

We have framed unpredicted persuasive results as the individual's expanded use of out-of-communication information to support flexible decision-making across contexts and time. While we view communicative persuasion as a form of knowledge-power relation, we emphasized that belief of such knowledge formed at one time can be different from the ones *accessible* at the point of performing the behavior (Conner & Norman, 2007). In this section, we discuss the psychology of such change of belief, which is necessary for further thinking the strategic use of different styles of behavioral theory and communication implementation towards lasting persuasive goals.

Whenever motivated, the once communicated and persuaded recipient could reflect on previously formed beliefs of knowledge with possible enhancing, diminishing, or modifying. Even when the same communication is repeated multiple times, different understandings of the same message might take into place. In this regard, it is not surprising that people can become less sensitized to secure behaviors with repeatedly presented ISec warnings (Amran et al., 2018; Vance et al., 2018). To gather out-of-communication information and knowledge

for decision-making support (shortening C-D gap), one may need time, resource, and motivation. In the following analysis on the psychology of time, we discuss how they are made more or less possible by different communication implementations.

In psychology, the process of belief was found to be a two-step process instead of just one step that simply yields "believing" or "not believing". While one tries to comprehend the information upon in contact with security communication (assuming she is motivated to process the message), it is straightforward to think that the process of believing happens after understanding. However, research suggest that, for the initial evaluation of information, understanding and believing happen in parallel at the same time. Specifically, the formation of human belief follows a *Spinozan procedure* (Gilbert, 1991), where the belief system first comprehends and accepts information. Only a little later, when more time allows the maneuver of mental resource, the second step kicks in and *certify or reject* the idea formulated, where additional information may be extracted from memory and the environment for supporting the operation of such certification or rejection. This could be the reason that the depletion of cognitive elaboration make people believe statements more easily instead of disabling their ability to neither accept or reject (e.g., believing at random level), even under conditions when participants have been told these statements were invalid beforehand (Silva, 2014). In other words, there is a natural inclination to believe any knowledge under conditions of simply limited time, which implies the inability to draw sufficient mental resource for certifying or rejecting.

Thus, at the moment of one-time communication delivery, *if the overall situation curbs and limits the happening of certification stage* (e.g., when the recipient needs to decide in seconds' situation based on available material), the communicative knowledge will be believed more easily, which is positive for candid persuasive effects or measurement, but leaves more room for unpredicted decision-making in the future where the individual could incorporate much different and varied information. In knowledge-power terms, shorter time implies that the decision-maker's inability in even initiating unpredicted decision-making since her information synthesis limited and belief easier to form solely based on the communication content available. While such condition tends to generate more predictable decision-making, it may also imply the lack of flexibility in generating varied understanding of the communication topic "deep" enough. For example, even if the individual only gets a sense of familiarity from the communication without any reflective understanding, preference and persuasive results could occur (Moons et al., 2009). If, on the other hand, situation permits and even enhances the evaluation of shortly-formed belief, the individual may be encouraged to discover, reflect and utilize more information sources and environmental variables to make sense of the "given" content (Olson & Clough, 2001), which may form somewhat reduced immediate persuasive effect but more resilient knowledge formations in a longer term.

Even if the belief and decision-making was carried out with full consideration around the time of communication delivery, it is still subject to

mutations caused by updated knowledge support the individual incorporates on the go, which could be referred to as the variations in elaboration likelihood (Petty & Cacioppo, 1986) where people engage in systematic or heuristic (Jacoby, 1991) reevaluations of issues whenever motivated. The validity of knowledge from the initial communication may only remain when it becomes the individual's normative knowledge for supporting given decision-making problems. It has a limited role when people engage in new decision-making evaluations which combines newer knowledge, and it may have an especially limited role when people engage in heuristic decision-making where they are once again under time pressure and limited access to mental resource (Chowdhury et al., 2019) in knowledge-power scenarios (i.e., the way a decision-making problem is presented) *not* similar to the initial communication. For example, when one gets an emergency call from a collogue asking for certain access to password that requires immediate decision-making, she may not utilize any of her knowledge from a previous communicative intervention to support the decision-making.

In this sense, the ISec theory and its communication application would only show higher predictive power on immediate response around the time of delivery under some kind of time pressure and mental resource limitation, as well as on future contexts where the individual rationally or heuristically chooses to consider similar knowledge to support decision-making (e.g., if the communication itself is a cued training on decision-making in expected situations such as standardized procedural knowledge/reflex training for handling emergency calls that requires system access override). For them to achieve improved predictive power, the communication implementation should encourage, rather than limit, the individual's ability in gathering information for decision-making at the time of communication delivery (although this shortens the C-D gap and could results in less predicted persuasive results at the time of persuasion). Alternatively, the behavioral theories themselves, should be combined, deconstructed, and tailored differently to different groups of people.

We illustrate both directions in the sections followed.

4.6 Implications on Behavioral Theories and Their Communicative Application

4.6.1 Implications on Utilizing Behavioral Theories

Afore-constructed analysis has rendered the applications of behavioral theories and their communicative implementation/presentation, while capable of explaining and predicting behaviors, also as psychological knowledges exerted to people (Henriques, 1998) that incites constrained thought processes which limit people's flexibility in making decisions. *Thus, the source of unpredictable behavioral persuasion results can be regarded as the restrained use of behavioral theory and excessive control of communicative implementation itself.*

Therefore, to theorize people's mental model of decision-making and results, the priority is to start from observations rather than fixating a viewpoint onto a particular theoretical ground. It is the flexible recombination of different theories that has more potential in explaining flexible decision-making processes across contexts where people freely choose different information for decision support. Since one could use different sets of information as decision support for similar problems, the modelling of "the change of behavioral pattern" may be needed, in which the same decision-making problem is explained by different theories in a set of different contexts. A meta-model may be put together by considering the probability of the occurrence of different contexts that involve the same ISec behavior along with the probability of the human agent's expected decision-making pattern in each type of context. With such modeling, long-term behavioral prediction and explanation may then be improved. However, this may require a large amount of data from the population, such as people's natural characteristics and classifications of different lifestyles and contexts, which bears statistical difficulty and ethical concerns (Grayson, 2008).

Furthermore, viewing theory and its communicative implementation as knowledge for temporary behavioral rules help us ask more diversified research questions, if not better ones. Questions such as "whether security campaign should be repeated" and "whether fear arousal is a must for fear appeal" is to be replaced by questions as "whether the persuasive power implication of the knowledge repeated in security campaign is consistent with individual's own extended information sources for decision-making support in other contexts" and "whether the information sources that contribute to the fear experience is also present in natural decision-making scenarios besides the fear appeal environment". Notice that the linguistic style of such shift of questioning arguably shows implied considerations for "a single truth for a single variable's effect" to "the consistency of truth's self-revealing across contexts".

4.6.2 Implications on ISec Communication Implementation

When aiming for long-term persuasive results, the communication implementation should be sensitive to the progression of individual's information gathering for decision-making over time and across contexts, rather than fitting people to static decision-maker's profiles incapable of rotating decision supports. The required communication design could dynamically enhance (rather than curb) the decision-maker's ability in gathering extended information and knowledge for supporting individualized decision-making (shortening C-D gap), which is of differed design philosophy compared to previously proposed time-and-resource-indifferent security training design methods based on supposed profiles of user's role, type of technology, risk of threat, etc. (De Keukelaere et al., 2009; Mangold, 2012).

Potential means of achieving such decision-making support could be manifold, such as presenting counter-arguments (e.g., showing opposite opinions against the security recommendation), motivating the individual's active reflection on the communication (e.g., asking them to think of counter-

arguments for the action recommendation), and promoting their access to out-of-communication information sources (e.g., providing means that allow the user to easily search extra information for decision-making support fitted to their own reflective thinking). Meanwhile, it could also responsively present follow-up persuasive contents as response to the information generated by the individual. In a smarter theory-based communication environment (e.g., an interactive educational program on ISec training), the communication should incorporate the user-generated information in the communication's original content, hence relating them to the theory that is most likely to explain such concerns, then dynamically present argument and other persuasive materials targeting individual user's self-generated information concern. In simple words, always asking for counterarguments and concerns from different knowledge and information sources before measuring the final persuasive effects.

Perhaps eventually, the co-creation of communicative content (e.g., arguments that support specific security recommendation) can be considered based on the difference between intended knowledge and normative knowledge in other contexts of a recipient's life. Suppose a piece of relevant knowledge that an individual's normative environment intends to promote is N, and the knowledge belief the communication intend to produce is B (e.g., ransomware is serious and worth preventing by installing anti-virus software). If B and N do not align with each other, then B must be resilient enough so that during long-term elaboration one may reject N and replace B with N (e.g., N is actually problematic), reinterpret N as aligned with B (e.g., ransomware is not a serious issue if one only uses a computer for entertainment), or reinterpret N as qualitatively different from B (e.g., the ransomware described in N is actually a different type of threat than that defined in B). Otherwise, B may be later unexpectedly rejected from the communication issuer's view. Alternatively, there could be modifications to both C and N so that they coexist without immediate issue. For example, one may resolve potential cognitive dissonance (Elliot & Patricia, 1994) by considering ransomware as only serious when the computer is used for financial purposes.

However, if the need for persuasive validity is short (e.g., target behavior only needs to be carried out once at the time of communication delivery) and the goal of communication is only to have the individual committed to a specific response for a specific threatening event (e.g., download and install a particular anti-malware software with clear instructions for a one-time malware scan), a straightforward communicative message that limits people's ability in information gathering may work better. When the necessary decision validity needed is long (e.g., long-term regular security checks in a system), but if the recommended behavior is clearly instructional and the behavior is only relevant to a specific context, such limited communicative implemented may also work better. On this account, there may be often a tradeoff between immediate effectiveness and stability. *More thorough elaborations of the communication content could mean higher rejection rates and lower overall immediate efficiency*. However, when extended information is set into place for decision-support, decision-making results may be more stable in the future. For example, security experts

may relate to more information from past experience even when prompted to make quick decisions on handling a security warning, and that decision may be more stable and less likely to be reverted in the future. However, they may also be *more critical* about the warning if the communication content is not in accord with their normative (also professional in this case) belief.

In turn, for conducting research designs in behavioral ISec, the considerations of C-D gap can be at least translated into conceptual and empirical studies on the variation, progression, decision-making outcome, and manipulation of factors and topics such as compulsory/free-form decision-making time (Chowdhury et al. 2019 also suggested the topic of time pressure from the viewpoint of cognitive load), individualized adaptive security awareness training based on counter-argument prompts, trade-off between decision stability and information richness, pre-existing security-related knowledge, communicative format designs that enhances decision-maker's active search of extra informational support during communication, user taxonomy based on decision variation over time instead of their role within organization, and so on.

In sum, we evaluate long-term communicative persuasion in relation to the enlargement or reduction of C-D gap with the variations in decision time and individual's active access to out-of-context information for candid decision support. For some problems, the communication may selectively present information to promote maximum short-term coping rates. In others, communication may attempt to increase people's *reflection* of matter by not only portraying one preset of theory-based of communication, but also promoting extra information gathering and dynamically adjusting response.

4.6.3 Implications on Reinterpreting Existing Studies

Our view on communication intervention as knowledge-power relations for decision-making support implies reinterpretation of existing studies on ISec intervention results, which is not adequate to be framed in the typical "independent-antecedent-to-dependent-effect" type of research flow.

If empirical research suggest a lack of lasting effects from fear appeals (Mwagwabi, 2015), it could imply that people's overall information support for long-term decision-making should not be approximated as the factors and their derived knowledge from what is described and developed from fear appeal theories, or that such information would only be relevant for decision-making under selective contexts. For instance, while PMT's applicability to ISec behaviors varies significantly in organizational or personal contexts (Posey et al., 2015), we may say that people make decisions based on information more aligned with what PMT-derived fear appeal contains in organizational settings, but much less in home settings.

Moody et al. (2018) derived a unified model of information security policy compliance based on a number of different risk avoidance theories IS. They addressed one of the limitations to be the data-driven statistical method which merged data modelled by different risk avoidance theories with inconsistent

theoretical assumptions. However, we view the statistical unification an attempt to identify characteristic factors in the recipient's long-term environment that contribute to decision-making. *If similar studies could be repeated at later times, we may infer how people's overall mental model of risk avoidance changes over time and across different contexts*. The data-driven approach is not a limitation, but an asset to explore the characteristic shift in post-reception normative environment under specific contexts. These results are valuable for long-term intervention implementations for statistical significance. If multiple communications are possible, the match between recipient's varied decision-making patterns with different communication implementation may be identified. When multiple communication is implausible, one-time delivery could be issued while considering the set of information that would be most relevant to them across different contexts.

Varied version of a theory or a component from a theory could be drawn based on how certain information is processed, understood and developed for decision support on the user's side. For example, although self-efficacy has been found to be positively correlated with coping assessment and intention, it should not exceed certain limit where unrealistic optimism could lead to disappointment and harm in the future (Conner & Norman, 2007). Thus, the distinction between pre-action self-efficacy, maintenance self-efficacy and recovery self-efficacy could be made as a further development of the concept of general self-efficacy (Luszczynska & Schwarzer, 2003). Relating to our framework, if pre-action self-efficacy resembles more of the initial belief of knowledge of self-efficacy, maintenance self-efficacy may involve more elaborated evaluation of behavioral hinderance during subsequent coping experience, and recovery self-efficacy informs the aftermath reevaluated self-efficacy while the problem has been solved.

4.7 Limitations

Our analysis has emphasized on the communication as knowledge and information for more or less flexible decision-making support, which portrays the level of unpredictability in persuasive results. We downplayed the role of immediate behavioral metrics such as action intention but highlighted the role of belief of knowledge and information in communicative intervention and decision-making. While it is possible to dissect the concept of belief and its relationship with intention (Eric, 2019), for the scope of our study, belief is a broad mental process involving the representation and assessment of any meaningful information (Radu J., 1986). By assumption, it should happen prior to behavioral intention. However, we acknowledge that it may be possible to affect intention without the influence of meaningful communication (e.g., change of intention from subliminal priming). It would be also possible to trigger behavioral change without first having any intention formed (e.g., if a warning window accompanied by loud sound triggers reflexive response to turn it off).

Our analysis is also somewhat ambiguous in directing very detailed evaluation the communication effectiveness. We view communication results as not as the measurement of behavioral compliance such as intention and coping rates, but ignorance or consideration of individual's active information search for decision-making support, which informs two basic strategies (information controlled vs. information enhanced) in communication implementation. Eventually, identifying which kind of communication works better would in which specific contexts would require empirical evidence gathering and professional design implementation with decent user experience.

4.8 Conclusion of Study 3

We assume a fully rational human's behavior as inherently unpredictable, and the level of such predictability varies with the closing or shortening of C-D gap, where the more information sources an individual utilizes for decision-making, the more unpredictable the results should be. Further, we view behavioral theory and its communicative implementation the production of knowledge presentation which carries persuasive power. Together, we discuss its implications on the flexible understanding and use of behavioral theory, and envision two general strategies of communicative implementation, where one strategy involves the controlled presentation of information knowledge, and the other promotes individual's integration of multiple information sources.

Overall, we wish our analysis of behavioral unpredictability assist in IS research's flexible use of behavioral theory and experiment in implementing information promoting ISec communication that potentially lasts better over time.

5 CONTRIBUTIONS

Knowledge pieces from different realms depend upon each other, and we often run a risk of relying on uninspected assumptions as well as authorities (Hardwig, 1985) while referring to seemingly straightforward concepts and ideas. Revisits of aforementioned human factors do not only benefit how an IS scholar models human risk perception, but also enrich the choices of persuasive strategy and research methodology in practice. The three studies presented in my dissertation have their respective contributions to MIS literature, as well as implications as a whole.

First of all, in Study 1, we empirically addressed the role of familiarity in ISec communication and traced its divergent effects in different contexts. This raises an alarm concerning superficially positive results, such that simply being familiar or overly familiar with ISec topics may imply negative sides for actual behavior while keeping a decent face-value risk perception. Method-wise, the novel use of a psychological experiment contributes to the available toolsets in the MIS methods arena. The study, with 32 different ISec threats implemented, also bridges the critical gap between general risk perception and specific perceptions towards individual threats. In practice, the results suggest that we may adapt different strategies in communicating ISec risks to the public, such that it could depend on the audience's preexisting level of familiarity with threats and the type of threat in focus. Perhaps more importantly for the integrity of my PhD research, this result also leaves a hint on the irreplaceable importance of genuine understanding as a basis for justified information security communication, as posed to behavioral nudging techniques in awareness campaigns that may only achieve accumulated repetitions of awareness.

If familiarity is at the foundation of the individual's ISec communication experience, "fear" could be argued as the core. While it feels natural to call anything we want to avoid as something we "fear", our discussions in Study 2 problematize and deepen the understanding of fear for MIS. We analyzed the multi-faceted nature of fear based on recent studies and discourses in psychology, where I argue what MIS researchers all label "fear" can mean very different processes in research and practice, and that a so-called objective measurement of

neural activities may not be the fundamental benchmark after all, especially in relation to IS's practical purposes. Such discussion contributes to general MIS research, in that the more we realize the diversity of fear across contexts, the more researchers are justified to abandon dogmatic measurements of affect and somewhat forced quantitative comparison of research results with different inherent qualities. Eventually, I propose the most important discursive effort in fear-related ISec research, not as a construct or term explained in quantitative modeling, but first and foremost a range of elaborated description of the specific phenomenon at hand.

The last piece of puzzle pays respect to the simple human capacity of engaging "a change of mind". Regardless of how one experiences ISec communication at first sight, there is a chance that they may think and behave differently in the future, which yields a different decision-making result in longer terms. If the discussion of familiarity and fear concerns the "here" and "now" as one *is* receiving persuasive communication, I stretch the axis of time here by discussing how an individual possibly change their mind after the initial persuasion. With two streams of thoughts in economics and philosophy, I suggest a framework which holds the capacity to explain unpredicted outcomes of decision-making while further reflecting on the rigorous use of behavioral theories in MIS, with which I flip and turn the assumed cause of insecure or deviant security behaviors, from the human agent's not being able to rationally realize a clear-cut threatening situation that requires rational protection, to the behavioral intervention's inability to consider and promote the recipient's sufficient elaboration and reflection of a bigger risk avoidance picture. For research, this discussion strongly justifies the flexible use of behavioral theories across time and contexts. For practice, it proposes two general strategies of communicative design for ISec, where one *controls* information and the other *opens up* information support for enhancing the independent user's lasting decision-making rationale.

Finally, I argue that the dissertation, viewing as a whole, contributes the most to the realization of "change" and "difference" for MIS. While science often attempts to discover patterns and simplify the world of complex happenings and noises into models of certainty, deconstruction of established patterns and beliefs is one important step toward complicating as well as understanding the theoretical simplicity in the ideal world. In this regard, the discussions of three seemingly "irrational" human aspects in ISec persuasive communications, namely *familiarity*, *fear*, and *a change of mind*, may be the key to understand and apply research models for human-centered ISec communication solutions in practice. If the aim of the "management" part of MIS is to shape expected behavior in organizations and public spheres, the acknowledgement of unexpected human mental capabilities in flux shall be the key to achieve a balance when unpredictability is unavoidable in a world of constant change.

6 CONCLUSION

In this dissertation, I explore three seemingly irrational human aspects in persuasive information security communication, namely familiarity, fear, and a change of mind. In my field of vision, they are some of the most important humane topics that need to be clarified before more studies are carried out based on established research methods and modes of thought in behavioral ISec research. Familiarity is at the foundation of the persuasive experience since ISec communication always familiarizes people with contents on threats regardless of the designed intention. Fear is at the core of the coping response as we intuitively assume that people avoid things they are afraid of. Further, regardless of any current experience and decision-making result, an individual can always have a change of mind along the axis of time.

Study 1 shows that familiarity may yield either positive or negative effect depending on the operationalization in communicative presentation, which indicates varied strategies for implementing ISec campaign based on audience's pre-existing level of familiarity and type of threats of interest. Study 2 dissects a multi-faceted notion of fear, where an emergingly rigid view of fear and its measurement in MIS is put into doubt. It suggests that the inherent meaning of the same mental construct can vary greatly across contexts, which could grant more freedom in the study of emotions and affects for MIS. Further, in Study 3, I construct a framework that portrays the human capability of having "a change of mind", where persuasive ISec communication is viewed not as a management instrument that guarantees persuasive results, but a comprehensive body of knowledge and information for individual's rational yet flexible decision-making support.

Together, this dissertation offers an understanding of the independent and flexible side of human mental capability in response to changing situations. If I were to summarize the implications in two takeaways for research and practice, it would be the following. In research, we could benefit from an intentional shift of modeling theoretical relationships among constructs, to better describing and maintaining the consistency of the actual phenomenon to be studied. In practice, we may achieve more resilient ISec interventions that promote individual's self-

reflection of risk avoidance situations as well as their independent decision-making process, rather than reaching immediate yet possibly superficial results by taking advantage of nudging techniques irrelevant to genuine understanding.

As last, I sincerely wish this dissertation would incite future discussions and impact human-centered ISec communication solutions in MIS.

YHTEENVETO (SUMMARY IN FINNISH)

Tässä tutkielmassa tarkastellaan kolmea irrationaalista inhimillistä tekijää tietoturvallisuusviestinnässä, turvallisuusuhkien tuttuutta, IT-aiheisten ärsykkeiden pelkoa ja inhimillistä kykyä muuttaa mieltä päätöksentekoprosessissa. Näiden tekijöiden merkitystä käsitellään erikseen ja yhdessä. Mikä tahansa tietoturvallinen (ISec) viestintä voi perehdyttää ihmisiä tiettyyn IT-uhkiin liittyvään sisältöön aiotusta tavoitteesta tai ei-toivotusta vaikutuksesta riippumatta. Perehtymisen jälkeen pelko voi olla selviytymisreaktion ytimessä, sillä ihmiset vain välttävät asioita, joita he pelkäävät. Lisäksi riippumatta alkuperäisistä päätöksentekotuloksista yksilö voi aina muuttaa mieltään tulevaisuudessa. Tässä mielessä tuttuus, pelko ja mielenmuutos käsitellään keskeisinä psykologisina tekijöinä kommunikaatiokontaktin alussa, päätöksenteon aikana ja mahdollisessa tulevaisuudessa, jossa päätöksenteon uudelleenkäynti tapahtuu. Selitän kolmella tutkimuksella kolme tekijää ja tutkin MIS-tutkimuskäytännössä huomiotta jätettyjä näkökohtia.

Tutkimus 1 osoittaa, että tuttuus voi tuottaa joko positiivisia tai negatiivisia vaikutuksia riippuen siitä, miten se toteutuu kommunikatiivisessa esityksessä. Tämä puoltaa ISec-kampanjan toteuttamisessa erilaisia strategioita, jotka perustuvat yleisön jo olemassa olevaan tuntemustasoon ja huomion kohteena olevien uhkien tyyppiin. Tutkimus 2 ehdotti monitahoista pelon ymmärtämistä vastakohtana jäykkään näkemykseen pelosta ja sen mittaamisesta johdon tietojärjestelmissä (MIS). Kuvaus saavuttaa kriittisen argumentin, jonka mukaan MIS:n tulisi lieventää painotusta standardoituun rakentamiseen ja mittaukseen, mikä puolestaan antaa enemmän vapautta ja kontekstualisoitua tarkkuutta tutkimuskäytännöissä. Tutkimuksessa 3 rakennetaan viitekehys, joka selittää, kuinka yksilöt voivat muuttaa mieltään alkuperäisten päätösten jälkeen. Se tiivistää olemuksen siitä, miksi turvallisuusviestintä voi epäonnistua pitkällä aikavälillä, ja ehdottaa edelleen poliittista sopivuutta, jossa ISec-viestintää ei voida hyödyntää johtamisvälineenä välittömän vakuuttavan vaikutuksen saavuttamiseksi vaan kokonaisvaltaisena tietona yksilön omaa päätöksentekoa tukemaan.

Kokonaisuudessaan väitöskirjassa pohditaan ihmisen henkisen kyvyn joustavaa luonnetta reagoida muuttuviin tilanteisiin. Se tukee näkökulmaa ihmisen jatkuvasti muuttuvista mielen rakenteista ja ehdottaa joustavampaa ja ihmiskeskeisempää ISec-viestintätyyliä, jossa yksilön henkisen tilan ja kommunikatiivisen suunnittelun välistä johdonmukaisuutta arvostetaan ja jossa riippumaton päätöksentekijä on vapaa käyttäytymiseen liittyvistä todellisen ymmärryksen kannalta merkityksettömistä suostuttelutekniikoista.

REFERENCES

2021 Data Breach Investigations Report. (2021). Verizon.

Abraham, C., & Michie, S. (2008). A taxonomy of behavior change techniques used in interventions. *Health Psychology*, *27*(3), 379–387. https://doi.org/10.1037/0278-6133.27.3.379

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior* (Pbk. ed). Prentice-Hall.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003

Allen, M. (2017). *The SAGE Encyclopedia of Communication Research Methods*. SAGE Publications, Inc. https://doi.org/10.4135/9781483381411

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. *IEEE Access*, *7*, 111341–111354. https://doi.org/10.1109/ACCESS.2019.2904006

Amran, A., Zaaba, Z. F., & Mahinderjit Singh, M. K. (2018). Habituation effects in computer security warning. *Information Security Journal: A Global Perspective*, *27*(2), 119–131. https://doi.org/10.1080/19393555.2018.1448492

Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015). How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2883–2892. https://doi.org/10.1145/2702123.2702322

Anderson, B., Bjornn, D., Jenkins, J., Kirwan, B., & Vance, A. (2018). *Improving Security Message Adherence through Improved Comprehension: Neural and Behavioral Insights*. 5.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Anderson, J. R., Reder, L. M., & Lebiere, C. (1996). Working Memory: Activation Limitations on Retrieval. *Cognitive Psychology*, *30*(3), 221–256. https://doi.org/10.1006/cogp.1996.0007

Aurigemma, S., & Mattson, T. (2018). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. *Journal of the Association for Information Systems*, 45.

Bacon, F. T. (1979). Credibility of repeated statements: Memory for trivia. *Journal of Experimental Psychology: Human Learning and Memory*, *5*(3), 241–252. https://doi.org/10.1037/0278-7393.5.3.241

Baddeley, A. (1992). Working memory. *Science*, *255*(5044), 556–559. https://doi.org/10.1126/science.1736359

Barrett, L. F. (2009). Variety is the spice of life: A psychological construction approach to understanding variability in emotion. *Cognition & Emotion*, *23*(7), 1284–1306. https://doi.org/10.1080/02699930902985894

Bartolomeo, P. (2008). The neural correlates of visual mental imagery: An ongoing debate. *Cortex*, *44*(2), 107–108. https://doi.org/10.1016/j.cortex.2006.07.001

Baskerville, R. L. (2002). *Information Systems as a Reference Discipline*. 1–14.

Beedie, C., Terry, P., & Lane, A. (2005). Distinctions between emotion and mood. *Cognition & Emotion*, *19*(6), 847–878. https://doi.org/10.1080/02699930541000057

Bellemare, C., Bissonnette, L., & Krrger, S. (2014). Statistical Power of within and Between-Subjects Designs in Economic Experiments. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3149007

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bradley, M. M., & Lang, P. J. (2007). Emotion and Motivation. In J. T. Cacioppo, L. G. Tassinary, & G. Berntson (Eds.), *Handbook of Psychophysiology* (3rd ed., pp. 581–607). Cambridge University Press. https://doi.org/10.1017/CBO9780511546396.025

Bravo-Lillo, C. A. (2014). *Improving Computer Security Dialogs: An Exploration of Attention and Habituation* [Doctoral dissertation, Carnegie Mellon University]. https://doi.org/10.1184/R1/6719972.v1

Brincat, S. L., & Connor, C. E. (2004). Underlying principles of visual shape selectivity in posterior inferotemporal cortex. *Nature Neuroscience*, *7*(8), 880–886. https://doi.org/10.1038/nn1278

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364–390. https://doi.org/10.1057/ejis.2015.21

Campbell, M. C., & Keller, K. L. (2003). Brand Familiarity and Advertising Repetition Effects. *Journal of Consumer Research*, *30*(2), 292–304. https://doi.org/10.1086/376800

Campos, J. J., Campos, R. G., & Barrett, K. C. (1989). Emergent Themes in the Study of Emotional Development and Emotion Regulation. *Developmental Psychology*, *25*(3), 394–402.

Casper, K. (2001). Affective feelings as feedback: Some cognitive consequences. *Theories of Mood and Cognition: A User's Guidebook*, *27*.

Chen, M.-F. (2016). Extending the protection motivation theory model to predict public safe food choice behavioural intentions in Taiwan. *Food Control*, *68*, 145–152. https://doi.org/10.1016/j.foodcont.2016.03.041

Chicken, J. C., & Posner, T. (1998). *The philosophy of risk*. Thomas Telford.

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review.

Behaviour & Information Technology, *38*(12), 1290–1308. https://doi.org/10.1080/0144929X.2019.1583769
Christensen, M. S., Ramsøy, T. Z., Lund, T. E., Madsen, K. H., & Rowe, J. B. (2006). An fMRI study of the neural correlates of graded visual perception. *NeuroImage*, *31*(4), 1711–1725. https://doi.org/10.1016/j.neuroimage.2006.02.023
Clark-Polner, E., Wager, T. D., Satpute, A. B., & Barrett, L. F. (2016). Neural fingerprinting: Meta-analysis, variation, and the search for brain-based essences in the science of emotion. In *Handbook of Emotions* (4th ed.). Guilford New York, NY.
Clore, G. L., & Schiller, A. J. (2016). New light on the affect-cognition connection. In *Handbook of Emotions* (pp. 532–546). Guilford Press New York.
Clore, G. L., Schiller, A. J., & Shaked, A. (2018). Affect and cognition: Three principles. *Current Opinion in Behavioral Sciences*, *19*, 78–82. https://doi.org/10.1016/j.cobeha.2017.11.010
Conner, M., & Norman, P. (Eds.). (2007). *Predicting health behaviour: Research and practice with social cognition models* (2. ed., repr). Open Univ. Press.
Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003
Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521–549. https://doi.org/10.1111/isj.12319
Cranor, L. F. (2008). A Framework for Reasoning About the Human in the Loop. *Proceedings of the 1st Conference on Usability, Psychology, and Security*, 1–15.
Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010
D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210
Davidson, K. W., Goldstein, M., Kaplan, R. M., Kaufmann, P. G., Knatterud, G. L., Orleans, C. T., Spring, B., Trudeau, K. J., & Whitlock, E. P. (2003). Evidence-based behavioral medicine: What is it and how do we achieve it? *Annals of Behavioral Medicine*, *26*(3), 161–171. https://doi.org/10.1207/S15324796ABM2603_01
De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., & Zurko, M. E. (2009). Adaptive Security Dialogs for Improved Security Behavior of Users. In T. Gross, J. Gulliksen, P. Kotzé, L. Oestreicher, P. Palanque, R. O. Prates, & M. Winckler (Eds.), *Human-Computer Interaction – INTERACT*

2009 (Vol. 5726, pp. 510–523). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03655-2_57
Debord, G. (1994). *The society of the spectacle*. Zone Books.
Dennis, A. R., & Minas, R. K. (2018). Security on Autopilot: Why Current Security Theories Hijack our Thinking and Lead Us Astray. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(SI), 15–38. https://doi.org/10.1145/3210530.3210533
Dillard, J. P. (1994). Rethinkin the Study of Fear Appeals: An Emotional Perspective. *Communication Theory*, *4*(4), 295–323. https://doi.org/10.1111/j.1468-2885.1994.tb00094.x
Elliot, A. J., & Patricia, G. Devine. (1994). On the motivational nature of cognitive dissonance: Dissonance as psychological discomfort. *Journal of Personality and Social Psychology*, *67*(3), 382–394.
Ellsworth, P. C., & Smith, C. A. (1988). From Appraisal to Emotion—Differences Among Unpleasant Feelings. *Motivation and Emotion*, *12*(3), 271–302.
Eric, S. (2019). Belief. In *The Stanford Encyclopedia of Philosophy* (Fall 2019). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2019/entries/belief/
Faizi, S. M., & Rahman, S. S. M. (2020). Effect of Fear on Behavioral Intention to Comply. *Proceedings of the 2020 the 4th International Conference on Information System and Data Mining*, 65–70. https://doi.org/10.1145/3404663.3404685
Fang, X., & Lee, S. (2016). Comparative Empirical Analysis on Computer Software Piracy Behaviors between China and the United States: An Exploratory Study. *Journal of International Technology and Information Management*, *25*(2), 21.
Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x
Folkman, S., & Lazarus, Ri. S. (1980). An Analysis of Coping in a Middle-Aged Community Sample. *Journal of Health and Social Behavior*, 22.
Foucault, M. (2007). *Security, Territory, Population: Lectures at the Collège de France, 1977-78*. Springer.
Foucault, M., Arnold, I. D., & Graham, B. (2008). *The birth of biopolitics: Lectures at the Collège de France, 1978-1979*. Springer.
Foucault, M., Bertani, M., Fontana, A., Ewald, F., & Macey, D. (2003). *Society must be defended: Lectures at the Collège de France, 1975-76* (1st ed). Picador.
Foucault, M., & Gordon, C. (1980). *Power/knowledge: Selected interviews and other writings, 1972-1977* (1st American ed). Pantheon Books.
Garcia-Marques, T. (2000). The positive feeling of familiarity: Mood as an information processing regulation mechanism. In *The message within: The role of subjective experience in social cognition and behavior* (pp. 240–261).
Garcia-Marques, T., & Mackie, D. M. (2001). The Feeling of Familiarity as a Regulator of Persuasive Processing. *Social Cognition*, *19*(1), 9–34. https://doi.org/10.1521/soco.19.1.9.18959

Garg, V., & Camp, J. (2012). End User Perception of Online Risk under Uncertainty. *2012 45th Hawaii International Conference on System Sciences*, 3278–3287. https://doi.org/10.1109/HICSS.2012.245
Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier.
Gilbert, D. T. (1991). How mental systems believe. *American Psychologist*, *46*(2), 107–119. https://doi.org/10.1037/0003-066X.46.2.107
Gilboa, I., & Schmeidler, D. (1995). Case-Based Decision Theory. *The Quarterly Journal of Economics*, *110*(3), 605–639. https://doi.org/10.2307/2946694
Gillebaart, M., Förster, J., & Rotteveel, M. (2012). Mere exposure revisited: The influence of growth versus security cues on evaluations of novel and familiar stimuli. *Journal of Experimental Psychology: General*, *141*(4), 699–714. https://doi.org/10.1037/a0027612
Gothard, K. M. (2020). *Multidimensional processing in the amygdala*. 27.
Grant, D. A. (1948). The latin square principle in the design and analysis of psychological experiments. *Psychological Bulletin*, *45*(5), 427–442. https://doi.org/10.1037/h0053912
Grayson, K. (2008). Human security as power/knowledge: The biopolitics of a definitional debate. *Cambridge Review of International Affairs*, *21*(3), 383–401. https://doi.org/10.1080/09557570802253625
Greenwald, A. G., & Sakumura, J. S. (1967). Attitude and selective learning: Where are the phenomena of yesteryear? *Journal of Personality and Social Psychology*, *7*(4, Pt.1), 387–397. https://doi.org/10.1037/h0025229
Gregor. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611. https://doi.org/10.2307/25148742
Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(2), 25–67.
Hansson, S. O. (1999). A Philosophical Perspective on Risk. *Ambio*, *28*(6), 539–542.
Hansson, S. O. (2018). Risk. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2018). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/fall2018/entries/risk/
Hardwig, J. (1985). Epistemic Dependence. *The Journal of Philosophy*, *82*(7), 335–349.
Harris, P. L., de Rosnay, M., & Pons, F. (2016). Understanding Emotion. In *Handbook of Emotions* (4th ed., pp. 293–306).
Hayat, Z., Reeve, J., & Boutle, C. (2007). Ubiquitous security for ubiquitous computing. *Information Security Technical Report*, *12*(3), 172–178. https://doi.org/10.1016/j.istr.2007.05.002
Heidegger, M. (1977). *The question concerning technology, and other essays*. Garland Pub.
Heiner, R. A. (1983). The Origin of Predictable Behavior. *The American Economic Review*, *73*(4), 560–595.
Heiner, R. A. (1985). *Origin of Predictable Behavior: Further Modeling and Applications*. *75*(2), 391–396.

Heiner, R. A. (1989). The origin of predictable dynamic behavior. *Journal of Economic Behavior & Organization*, *12*(2), 233–257. https://doi.org/10.1016/0167-2681(89)90057-7

Hekkala, R., & Stein, M.-K. (2016). Silences and Voices of Fear, Anger, and Rationality: Emotionologies in an Information Systems Project. In N. M. Ashkanasy, C. E. J. Härtel, & W. J. Zerbe (Eds.), *Research on Emotion in Organizations* (Vol. 12, pp. 381–408). Emerald Group Publishing Limited. https://doi.org/10.1108/S1746-979120160000012012

Helm, B. W. (2010). Emotions and Motivation: Reconsidering Neo-Jamesian Accounts. In *The Oxford Handbook of Philosophy of Emotion* (pp. 303–323).

Henninger, F., Shevchenko, Y., Mertens, U., Kieslich, P. J., & Hilbig, B. E. (2019). *lab.js: A free, open, online experiment builder*. Zenodo. https://doi.org/10.5281/zenodo.597045

Henriques, J. (Ed.). (1998). *Changing the subject: Psychology, social regulation, and subjectivity*. Routledge.

Higbee, K. L. (1969). Fifteen years of fear arousal: Research on threat appeals: 1953-1968. *Psychological Bulletin*, *72*(6), 426–444. https://doi.org/10.1037/h0028430

Hsee, C. K., & Hastie, R. (2006). Decision and experience: Why don't we choose what makes us happy? *Trends in Cognitive Sciences*, *10*(1), 31–37. https://doi.org/10.1016/j.tics.2005.11.007

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2007). A Survey of Factors Influencing People's Perception of Information Security. In J. A. Jacko (Ed.), *Human-Computer Interaction. HCI Applications and Services* (Vol. 4553, pp. 906–915). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-73111-5_100

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221–232. https://doi.org/10.1080/01449290701679361

Hubert, M., Linzmajer, M., Riedl, R., Hubert, M., Kenning, P., & Weber, B. (2017). Using Psycho-physiological Interaction Analysis with fMRI Data in IS Research: A Guideline. *Communications of the Association for Information Systems*, *40*, 181–217. https://doi.org/10.17705/1CAIS.04009

Jacoby, L. L. (1991). A process dissociation framework: Separating automatic from intentional uses of memory. *Journal of Memory and Language*, *30*(5), 513–541. https://doi.org/10.1016/0749-596X(91)90025-F

Janak, P. H., & Tye, K. M. (2015). From circuits to behaviour in the amygdala. *Nature*, *517*(7534), 284–292. https://doi.org/10.1038/nature14188

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, *66*, 129–141. https://doi.org/10.1016/j.cose.2017.01.010

Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, *45*(1), 20–31. https://doi.org/10.1037/0022-3514.45.1.20

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their Language: Designing Effective Messages to Improve Employees'

Information Security Decision Making. *Decision Sciences*, *50*(2), 245–284. https://doi.org/10.1111/deci.12328
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, *39*(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06
Johnston & Warkentin. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549. https://doi.org/10.2307/25750691
Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*, *30*(2), 687–704. https://doi.org/10.1287/isre.2018.0827
Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security*, *93*, 101782. https://doi.org/10.1016/j.cose.2020.101782
Keen, P. G. (1980). *MIS research: Reference disciplines and a cumulative tradition*. 12.
Keller, P. A., & Block, L. G. (1996). Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration. *Journal of Consumer Research*, *22*(4), 448–459.
Kerlinger, F. N. (1986). *Foundations of behavioral research*. New York: Holt, Rinehart and Winston.
Kessels, L. T. E., Ruiter, R. A. C., & Jansma, B. M. (2010). Increased attention but more efficient disengagement: Neuroscientific evidence for defensive processing of threatening health information. *Health Psychology*, *29*(4), 346–354. https://doi.org/10.1037/a0019372
Kim, M. J., Loucks, R. A., Palmer, A. L., Brown, A. C., Solomon, K. M., Marchante, A. N., & Whalen, P. J. (2011). The structural and functional connectivity of the amygdala: From normal emotion to pathological anxiety. *Behavioural Brain Research*, *223*(2), 403–410. https://doi.org/10.1016/j.bbr.2011.04.025
Kunda, Z. (1987). Motivated inference: Self-serving generation and evaluation of causal theories. *Journal of Personality and Social Psychology*, *53*(4), 636–647. https://doi.org/10.1037/0022-3514.53.4.636
Kuppens, P., Mechelen, I. V., Smits, D. J. M., & Boeck, P. D. (2003). The Appraisal Basis of Anger: Specificity, Necessity, and Sufficiency of Components. *Emotion*, *3*(3), 254–269.
Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping* (11. [print.]). Springer.
LeDoux, J. E. (2008). Emotional colouration of consciousness: How feelings come about. *Frontiers of Consciousness: Chichele Lectures*, 69–130.
Lee, J. K., Park, J., Gregor, S., & Yoon, V. (2021). Axiomatic Theories and Improving the Relevance of Information Systems Research. *Information Systems Research*, *32*(1), 147–171. https://doi.org/10.1287/isre.2020.0958
Leik, R. K. (2013). The Basics of Experimental Design. In *Experimental Design and the Analysis of Variance*. https://dx.doi.org/10.4135/9781483348940

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. In *Advances in Experimental Social Psychology* (Vol. 5, pp. 119–186). Elsevier. https://doi.org/10.1016/S0065-2601(08)60091-X

Leventhal, H. (1971). Fear appeals and persuasion: The differentiation of a motivational construct. *American Journal of Public Health*, *61*(6), 1208–1224. https://doi.org/10.2105/AJPH.61.6.1208

Li, Y., & Siponen, M. (2011). A call for research on home users' information security behaviour. *PACIS 2011 Proceedings*, 112.

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. "Andy." (2019). What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective. *MIS Quarterly*, *43*(2), 373–394. https://doi.org/10.25300/MISQ/2019/14360

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

Liberman, A., & Chaiken, S. (1992). Defensive Processing of Personally Relevant Health Messages. *Personality and Social Psychology Bulletin*, *18*(6), 669–679. https://doi.org/10.1177/0146167292186002

Lidskog, R. (2013). Sociology of risk. In *Essentials of risk theory* (pp. 75–105). Springer.

Lindquist, K. A., Wager, T. D., Kober, H., Bliss-Moreau, E., & Barrett, L. F. (2012). The brain basis of emotion: A meta-analytic review. *Behavioral and Brain Sciences*, *35*(3), 121–143. https://doi.org/10.1017/S0140525X11000446

Lucassen, T., & Schraagen, J. M. (2010). Trust in wikipedia: How users trust information from an unknown source. *Proceedings of the 4th Workshop on Information Credibility - WICOW '10*, 19. https://doi.org/10.1145/1772938.1772944

Lundgren, R. E., & McMakin, A. H. (2018). *Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks*. John Wiley & Sons, Inc.

Luszczynska, A., & Schwarzer, R. (2003). Planning and Self-Efficacy in the Adoption and Maintenance of Breast Self-Examination: A Longitudinal Study on Self-Regulatory Cognitions. *Psychology & Health*, *18*(1), 93–108. https://doi.org/10.1080/0887044021000019358

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Mäenpää, K., Kale, S. H., Kuusela, H., & Mesiranta, N. (2008). Consumer perceptions of Internet banking in Finland: The moderating role of familiarity. *Journal of Retailing and Consumer Services*, *15*(4), 266–276. https://doi.org/10.1016/j.jretconser.2007.05.007

Mangold, L. V. (2012). Using Ontologies for Adaptive Information Security Training. *2012 Seventh International Conference on Availability, Reliability and Security*, 522–524. https://doi.org/10.1109/ARES.2012.52

McCoy, S., Everard, A., Galletta, D. F., & Moody, G. D. (2017). Here we go again! The impact of website ad repetition on recall, intrusiveness, attitudes, and site revisit intentions. *Information & Management*, *54*(1), 14–24. https://doi.org/10.1016/j.im.2016.03.005

McDermott, M. S., & Sharma, R. (2017). Evaluating the impact of method bias in health behaviour research: A meta-analytic examination of studies utilising the theories of reasoned action and planned behaviour. *Health Psychology Review*, *11*(4), 358–373. https://doi.org/10.1080/17437199.2017.1339568

Mechelli, A. (2004). Where Bottom-up Meets Top-down: Neuronal Interactions during Perception and Imagery. *Cerebral Cortex*, *14*(11), 1256–1265. https://doi.org/10.1093/cercor/bhh087

Medin, D., & Ortony, A. (1989). Comments on Part I: Psychological essentialism. In S. Vosniadou & A. Ortony (Eds.), *Similarity and Analogical Reasoning* (1st ed., pp. 179–196). Cambridge University Press. https://doi.org/10.1017/CBO9780511529863.009

Mendes, W. (2016). Emotion and the Autonomic Nervous System. In *Handbook of Emotions* (4th ed.). Guilford New York, NY.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Mewborn, C. R., & Rogers, R. W. (1979). Effects of threatening and reassuring components of fear appeals on physiological and verbal measures of emotion and attitudes. *Journal of Experimental Social Psychology*, *15*(3), 242–253. https://doi.org/10.1016/0022-1031(79)90035-0

Milosevic, I. (2015). Fight-or-flight response. *Phobias: The Psychology of Irrational Fear: The Psychology of Irrational Fear*, *196*, 179.

Montoya, R. M., Horton, R. S., Vevea, J. L., Citkowicz, M., & Lauber, E. A. (2017). A re-examination of the mere exposure effect: The influence of repeated exposure on recognition, familiarity, and liking. *Psychological Bulletin*, *143*(5), 459–498. https://doi.org/10.1037/bul0000085

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Moons, W. G., Mackie, D. M., & Garcia-Marques, T. (2009). The impact of repetition-induced familiarity on agreement with weak and strong arguments. *Journal of Personality and Social Psychology*, *96*(1), 32–44. https://doi.org/10.1037/a0013461

Mwagwabi, F. M. (2015). *A Protection Motivation Theory Approach to Improving Compliance with Password Guidelines*.

Nabi, R. L., & Nabi, R. L. (2014). Emotional Flow in Persuasive Health Messages. *Health Communication*, *30*(2), 114–124.

Nepomuceno, M. V., Laroche, M., & Richard, M.-O. (2014). How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns.

Journal of Retailing and Consumer Services, *21*(4), 619–629. https://doi.org/10.1016/j.jretconser.2013.11.006
Oatley, K., Parrott, W. G., Smith, C., & Watts, F. (2011). Cognition and Emotion over twenty-five years. *Cognition & Emotion*, *25*(8), 1341–1348.
Okasha, S. (2016). *Philosophy of Science: Very Short Introduction*. Oxford University Press.
Olson, J. K., & Clough, M. P. (2001). Technology's Tendency to Undermine Serious Study: A Cautionary Note. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, *75*(1), 8–13. https://doi.org/10.1080/00098650109599225
Olucha-Bordonau, F. E., Fortes-Marco, L., Otero-García, M., Lanuza, E., & Martínez-García, F. (2015). Amygdala. In *The Rat Nervous System* (pp. 441–490). Elsevier. https://doi.org/10.1016/B978-0-12-374245-2.00018-8
Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal Level Theory in the Design of Fear Appeals in IS Security Research. *Communications of the Association for Information Systems*, 15.
Ordoñana, J. R., González-Javier, F., Espín-López, L., & Gómez-Amor, J. (2009). Self-Report and Psychophysiological Responses to Fear Appeals. *Human Communication Research*, *35*(2), 195–220.
Ortiz, J., Resnick, M. L., & Kengskool, K. (2000). The Effects of Familiarity and Risk Perception on Workplace Warning Compliance. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *44*(28), 826–829. https://doi.org/10.1177/154193120004402811 5
Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004
Parkinson, B. (1997). Untangling the Appraisal-Emotion Connection. *Personality and Social Psychology Review*, *1*(1), 62–79. https://doi.org/10.1207/s15327957pspr0101_5
Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment* (p. 54).
Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In *Advances in Experimental Social Psychology* (Vol. 19, pp. 123–205). Elsevier. https://doi.org/10.1016/S0065-2601(08)60214-2
Podsakoff, N. P., Whiting, S. W., Welsh, D. T., & Mai, K. M. (2013). Surveying for "artifacts": The susceptibility of the OCB–performance evaluation relationship to common rater, item, and measurement context effects. *Journal of Applied Psychology*, *98*(5), 863–874. https://doi.org/10.1037/a0032588
Pollen, D. A. (1999). On the Neural Correlates of Visual Perception. *Cerebral Cortex*, *9*(1), 4–19. https://doi.org/10.1093/cercor/9.1.4
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

Postman, N. (1987). *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*. Methuen.
Postman, N. (2006). *Amusing ourselves to death: Public discourse in the age of show business* (20th anniversary ed). Penguin Books.
Puhakainen & Siponen. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757. https://doi.org/10.2307/25750704
Radu J., B. (1986). The importance of belief. In *Belief: Form, content, and function* (pp. 1–16).
Reinhard, M.-A., Schindler, S., Raabe, V., Stahlberg, D., & Messner, M. (2014). Less is sometimes more: How repetition of an antismoking advertisement affects attitudes toward smoking and source credibility. *Social Influence*, *9*(2), 116–132. https://doi.org/10.1080/15534510.2013.790839
Rhodes, N. (2017). Fear-Appeal Messages: Message Processing and Affective Attitudes. *Communication Research*, *44*(7), 952–975. https://doi.org/10.1177/0093650214565916
Riedl, R., Fischer, T., & Léger, P.-M. (2017). *A Decade of NeuroIS Research: Status Quo, Challenges, and Future Directions*. 29.
Riesch, H. (2013). Levels of Uncertainty. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), *Essentials of Risk Theory* (pp. 29–56). Springer Netherlands. https://doi.org/10.1007/978-94-007-5455-3_2
Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation theory. In *Social psychophysiology: A sourcebook* (pp. 153–176).
Rogers, R. W., & Mewborn, C. R. (1976). Fear Appeals and Attitude Change: Effects of a Threat's Noxiousness, Probability of Occurrence, and the Efficacy of Coping Responses. *Journal of Personality and Social Psychology*, 8.
Rogers, R. W., & Steven, P.-D. (1997). Protection motivation theory. In *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132).
Rohr, M., Degner, J., & Wentura, D. (2015). The "emotion misattribution" procedure: Processing beyond good and bad under masked and unmasked presentation conditions. *Cognition and Emotion*, *29*(2), 196–219. https://doi.org/10.1080/02699931.2014.898613
Roseman, I., & Evdokas, A. (2004). Appraisals cause experienced emotions: Experimental evidence. *Cognition & Emotion*, *18*(1), 1–28. https://doi.org/10.1080/02699930244000390
Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, *49*(2), 63–70. https://doi.org/10.1002/ijop.12042
Samsudin, N. F., Zaaba, Z. F., Singh, M. M., & Samsudin, A. (2016). Symbolism in Computer Security Warnings: Signal Icons and Signal Words. *International Journal of Advanced Computer Science and Applications*, *7*(10), 7.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). "Transforming the 'weakest link' — A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Schwarz, N. (2000). Emotion, cognition, and decision making. *Cognition & Emotion*, *14*(4), 433–440. https://doi.org/10.1080/026999300402745

Sergerie, K., Chochol, C., & Armony, J. L. (2008). The role of the amygdala in emotional processing: A quantitative meta-analysis of functional neuroimaging studies. *Neuroscience & Biobehavioral Reviews*, *32*(4), 811–830. https://doi.org/10.1016/j.neubiorev.2007.12.002

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Shi, J. (Jolie), & Smith, S. W. (2016). The effects of fear appeal message repetition on perceived threat, perceived efficacy, and behavioral intention in the extended parallel process model. *Health Communication*, *31*(3), 275–286. https://doi.org/10.1080/10410236.2014.948145

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Siegel, E. H., Sands, M. K., Van den Noortgate, W., Condon, P., Chang, Y., Dy, J., Quigley, K. S., & Barrett, L. F. (2018). Emotion fingerprints or emotion populations? A meta-analytic investigation of autonomic features of emotion categories. *Psychological Bulletin*, *144*(4), 343–393. https://doi.org/10.1037/bul0000128

Silva, R. R. D. (2014). *"The truth is never pure and rarely simple": Understanding the role of repetition and processing fluency on the illusion of truth effect* [ISPA - Instituto Universitário das Ciências Psicológicas, Sociais e da Vida]. http://hdl.handle.net/10400.12/3187

Siponen, M. (2001). Five dimensions of information security awareness. *SIGCAS Comput. Soc.*, *31*(2), 24–29.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Baskerville, R., & Georgia State University. (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. https://doi.org/10.17705/1jais.00491

Siponen, M., & Klaavuniemi, T. (2019). *Narrowing the Theory's or Study's Scope May Increase Practical Relevance*. 10.

Smith, C. A., & Ellsworth, P. C. (1985). Patterns of Cognitive Appraisal in Emotion. *Journal of Personality and Social Psychology*, *48*(4), 813–838.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., & Cranor, L. F. (2009). *Crying Wolf: An Empirical Study of SSL Warning Effectiveness*. 34.

Suvak, M. K., & Barrett, L. F. (2011). Considering PTSD from the perspective of brain processes: A psychological construction approach: The Psychological Construction of PTSD. *Journal of Traumatic Stress*, *24*(1), 3–24. https://doi.org/10.1002/jts.20618

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178–1204. https://doi.org/10.1037/a0039729

Tanner, K. (2002). Experimental research designs. In *Research Methods for Students, Academics and Professionals* (pp. 125–146). Elsevier. https://doi.org/10.1016/B978-1-876938-42-0.50015-0

Thomas, E. J., Webb, S., & Tweedie, J. (1961). Effects of familiarity with a controversial issue on acceptance of successive persuasive communications. *The Journal of Abnormal and Social Psychology*, *63*(3), 656–659. https://doi.org/10.1037/h0044797

Tiedens, L. Z., & Linton, S. (2001). Judgment under emotional certainty and uncertainty: The effects of specific emotions on information processing. *Journal of Personality and Social Psychology*, *81*(6), 973–988. https://doi.org/10.1037/0022-3514.81.6.973

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

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., Anderson, B., Brigham Young University, Kirwan, C. B., Brigham Young University, Eargle, D., & University of Pittsburgh. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), 679–722. https://doi.org/10.17705/1jais.00375

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments. *MIS Quarterly*, *42*(2), 355–380. https://doi.org/10.25300/MISQ/2018/14124

Wager, T. D., van Ast, V. A., Hughes, B. L., Davidson, M. L., Lindquist, M. A., & Ochsner, K. N. (2009). Brain mediators of cardiovascular responses to

social threat, Part II: Prefrontal-subcortical pathways and relationship with anxiety. *NeuroImage*, *47*(3), 836–851. https://doi.org/10.1016/j.neuroimage.2009.05.044

Wager, T. D., Waugh, C. E., Lindquist, M., Noll, D. C., Fredrickson, B. L., & Taylor, S. F. (2009). Brain mediators of cardiovascular responses to social threat, Part I: Reciprocal dorsal and ventral sub-regions of the medial prefrontal cortex and heart-rate reactivity. *NeuroImage*, *47*(3), 821–835. https://doi.org/10.1016/j.neuroimage.2009.05.043

Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*, 277–300. https://doi.org/10.17705/1CAIS.04113

Wall, J. D., & Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*. https://doi.org/10.1016/j.im.2019.03.002

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association of Information Systems*, *17*(3), 194–215.

Warkentin, M., Walden, E., Texas Tech University, Johnston, A., University of Alabama at Birmingham, Straub, D., Temple University, & Korea University Business School. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems*, *17*(3), 194–215. https://doi.org/10.17705/1jais.00424

Whittlesea, B. W. A., & Williams, L. D. (2000). The source of feelings of familiarity: The discrepancy-attribution hypothesis. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *26*(3), 547–565. https://doi.org/10.1037//0278-7393.26.3.547

Willcocks, L. (2004). Foucault, power/knowledge and information systems: Reconstructing the present. *Social Theory and Philosophy for Information Systems*, 238–296.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Yang, C.-G., & Lee, H.-J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, *18*(2), 253–263. https://doi.org/10.1007/s10796-015-9594-x

Yao, G., & Li, Q. (2008). The Impact of Familiarity and Reputation on Consumer Trust in E-Commerce. *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 1–5. https://doi.org/10.1109/WiCom.2008.2183

Zaaba, Z. F., & Boon, T. K. (2015). Examination on Usability Issues of Security Warning Dialogs. *Journal of Multidisciplinary Engineering Science and Technology*, *2*(6), 9.

Zokaei, N., Manohar, S., Husain, M., & Feredoes, E. (2014). Causal Evidence for a Privileged Working Memory State in Early Visual Cortex. *Journal of Neuroscience*, *34*(1), 158–162. https://doi.org/10.1523/JNEUROSCI.2899-13.2014