European Journal of Information Systems (2015) 00, 1–27
© 2015 Operational Research Society Ltd. All rights reserved 0960-085X/15
www.palgrave-journals.com/ejis/

RESEARCH ESSAY

How users perceive and respond to security messages: a NeuroIS research agenda and empirical study

Bonnie Brinton Anderson[1], Anthony Vance[1], C. Brock Kirwan[2], David Eargle[3] and Jeffrey L. Jenkins[1]

[1]Information Systems Department, Marriott School of Management, Brigham Young University, Provo, U.S.A.; [2]Department of Psychology and Neuroscience, Brigham Young University, Provo, U.S.A.; [3]Katz Graduate School of Business, University of Pittsburgh, U.S.A.

Correspondence: Anthony Vance, Information Systems Department, Brigham Young University, 779 TNRB, Provo, UT 84604, U.S.A.
Tel: +1 801 361 2531;
E-mail: anthony@vance.name

Abstract

Users are vital to the information security of organizations. In spite of technical safeguards, users make many critical security decisions. An example is users' responses to security messages – discrete communication designed to persuade users to either impair or improve their security status. Research shows that although users are highly susceptible to malicious messages (e.g., phishing attacks), they are highly resistant to protective messages such as security warnings. Research is therefore needed to better understand how users perceive and respond to security messages. In this article, we argue for the potential of NeuroIS – cognitive neuroscience applied to Information Systems – to shed new light on users' reception of security messages in the areas of (1) habituation, (2) stress, (3) fear, and (4) dual-task interference. We present an illustrative study that shows the value of using NeuroIS to investigate one of our research questions. This example uses eye tracking to gain unique insight into how habituation occurs when people repeatedly view security messages, allowing us to design more effective security messages. Our results indicate that the eye movement-based memory (EMM) effect is a cause of habituation to security messages – a phenomenon in which people unconsciously scrutinize stimuli that they have previously seen less than other stimuli. We show that after only a few exposures to a warning, this neurological aspect of habituation sets in rapidly, and continues with further repetitions. We also created a polymorphic warning that continually updates its appearance and found that it is effective in substantially reducing the rate of habituation as measured by the EMM effect. Our research agenda and empirical example demonstrate the promise of using NeuroIS to gain novel insight into users' responses to security messages that will encourage more secure user behaviors and facilitate more effective security message designs.

European Journal of Information Systems (2015) **0**(0), 1–27.
doi:10.1057/ejis.2015.21

Keywords: security messages; information security behavior; NeuroIS; habituation; dual-task interference; eye tracking

Introduction

In recent years, information security has emerged as a top managerial concern, driving the worldwide security technology and services market to a value of U.S.$67.2 billion in 2013, and it is expected to increase to $86 billion by 2016 (Gartner, 2013). Despite the growing investment in information security technology, users continue to represent the weakest link in

Received: 2 March 2014
Revised: 2 November 2015
Accepted: 10 November 2015

security (Furnell & Clarke, 2012). Accordingly, attackers increasingly target users to gain access to the information resources of organizations (Mandiant, 2013).

A crucial aspect of security behavior is how users perceive and respond to security messages – discrete communication designed to persuade users to either impair or improve their information security posture. Research shows that users are susceptible to malicious messages such as phishing attacks that prompt users to install malware or visit compromised Websites (Hong, 2012). A parallel stream of research shows that users routinely disregard protective messages such as software security warnings (Bravo-Lillo *et al*, 2013). One reason for the ineffectiveness of warnings is the mismatch between security concerns and security behavior. For example, individuals' stated security concerns have been found to be inconsistent with their subsequent behavior in response to security warnings (Vance *et al*, 2014). These empirical results confirm those of Crossler *et al* (2013), who called for research that explains the discrepancy between security intentions and behaviors.

One promising means for exploring the security intention–behavior disparity in the context of security messages is NeuroIS – cognitive neuroscience and its associated neurophysiological measures applied to information systems (Dimoka *et al*, 2011). The neural bases for human cognitive processes can offer new insights into the complex interaction between information processing and decision making (Dimoka *et al*, 2012), allowing researchers to open the 'black box' of cognition by directly observing the brain (Benbasat *et al*, 2010). The potential of NeuroIS has been recognized by security researchers who have begun using neurophysiological measures to investigate security behavior (e.g., Moody *et al*, 2011; Warkentin *et al*, 2012; Hu *et al*, 2014; Vance *et al*, 2014; Neupane *et al*, 2014, 2015). We term this approach neurosecurity (Anderson *et al*, 2015). Crossler *et al* (2013, p. 96) observed that 'these studies, and others like them, will offer new insights into individual behaviors and cognitions in the context of information security threats'.

In this article, we argue for the potential of NeuroIS to shed new light on users' reception of security messages. We contribute to the nascent area of NeuroIS security research by presenting a research agenda for examining cognitive and emotional responses to security messages. To do so, we outline four key questions drawn from the security and cognitive neuroscience literature that directly relate to how users receive and process security messages. NeuroIS theories and methodologies can help advance pressing needs in each of these areas, generating potentially fruitful streams of research. These are not the only important research questions, but they represent the security issues that NeuroIS is ideally suited to address. Therefore, our guiding questions for researching security messages via NeuroIS are:

1. How does habituation affect users' responses to security messages?
2. What is the impact of stress on a users' response to security messages?
3. How does fear influence users' cognitive processing of security messages?
4. How does dual-task interference, for example, multitasking, disrupt the cognitive processing of security messages?

To illustrate how NeuroIS can be used to advance these research questions, we present the results of an experiment that uses the NeuroIS method of eye tracking to begin exploring our first research question on habituation. Habituation as a mental state is difficult to observe using conventional methods. Therefore, security researchers have examined habituation indirectly by observing its influence on security behavior rather than by measuring habituation itself (e.g., Brustoloni & Villamarín-Salomón, 2007; Bravo-Lillo *et al*, 2013). Although valuable for highlighting the problem of habituation with regard to security warnings, these conventional methods do not provide insight into the neurological process of habituation, which could lead to more effective security message designs.

We illustrate the potential of NeuroIS to address this gap in two ways. First, using eye tracking to measure the eye movement-based memory (EMM) effect – a neurological phenomenon in which people unconsciously scrutinize images previously seen – we demonstrate how habituation develops in the brain. We show that after only a few exposures to a warning, habituation sets in rapidly and continues to decline with further repetitions. These results (a) reveal how quickly habituation to warnings develops over time, and (b) provide a neurobiological explanation for why it occurs – both contributions made possible through the application of NeuroIS.

Second, we use eye tracking to evaluate the effectiveness of a security message designed to reduce habituation, a polymorphic warning whose appearance changes with each exposure. Previous studies of habituation were limited in their efforts to design warnings that target habituation because they did not have the benefit of neurophysiological measures. Using eye-tracking measures of the EMM effect, we were able to directly measure whether a polymorphic warning was effective in reducing habituation. We found that people were substantially less habituated to polymorphic warnings compared with conventional warnings.

Our research agenda and illustrative experiment demonstrate the promise of using NeuroIS to study users' responses to security messages. We anticipate that the pursuit of this research agenda will provide scholars with a more complete understanding of how users neurologically process security messages, which will lead to the more accurate development and application of theory (Dimoka *et al*, 2011). We also expect that the neurophysiological data stemming from this research will guide the design and testing of more effective forms of security messages to mitigate security threats to users (Dimoka *et al*, 2012). This article echoes Crossler *et al* (2013) call to use NeuroIS methods to study information security behavior by identifying the insights that can be gained through neurophysiological methods.

This article is organized as follows. First, we formally define security messages and give a brief overview of NeuroIS methods. We then describe the literature review we performed to identify our research questions. Next, for each research question, we highlight (a) existing gaps in the security literature, and why these gaps are important to address, and (b) potential ways NeuroIS can be used to address these gaps. We then show the value of applying NeuroIS to investigate our research questions through an eye-tracking experiment. Finally, we describe the implications of our research agenda for future research on security messages.

Review of security messages and NeuroIS

Security messages

We define a security message as discrete communication that is designed to persuade users to either impair or improve their information security posture. Most security messages are predominantly textual, such as software dialogs or e-mail communication, but messages may be aural, visual, or both, such as voicemail memos, signage, or online videos. See Appendix A for a taxonomy of security messages. Our definition is broad in that it includes messages from both attackers and defenders because both commonly use the same persuasive techniques and cues (Dhamija *et al*, 2006; Abbasi *et al*, 2010; Bravo-Lillo *et al*, 2013), and engage many of the same mental processes (Wright & Marett, 2010; Luo *et al*, 2013). Our definition is narrow, though, because it includes only discrete messages, rather than the entirety of security-related communication. The latter typically includes interaction with coworkers and peers; security, education, training, and awareness (SETA); classroom instruction (Karjalainen & Siponen, 2011); and sustained social engineering attacks that might continue over hours, days, or longer (Mitnick & Simon, 2001).

The potential of NeuroIS to explain security behavior

As the field of information security behavior matures, understanding why a particular behavior happens becomes increasingly necessary. To this end, NeuroIS offers a promising approach for investigating the effectiveness of security (Crossler *et al*, 2013). The neural bases for human cognitive processes can offer new insights into the complex interactions among the processing of security messages, decision making, and behavior (Dimoka *et al*, 2011).

Whereas IS researchers have historically relied on external measures of cognition, such as survey responses or observed behavior, neuroscience methods allow researchers to open the 'black box' of cognition by directly observing brain processes (Benbasat *et al*, 2010). 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). The promise of applying neuroscience to Human Computer Interaction (HCI) is to use insights from research on neurological processes to design effective user interfaces that can help users make informed decisions (Mach *et al*, 2010; Riedl *et al*, 2010).

Table 1 presents a sampling of the variety of tools and measures available in NeuroIS, along with key citations for more information about each method. For further information, see Dimoka *et al* (2012) and Riedl *et al* (2014), who offer a thorough discussion of the methods, tools, and measurements associated with NeuroIS.

Identifying research questions for examining users' reception of security messages through the lens of NeuroIS

To select questions for our research agenda, we took a three-pronged approach by analyzing (1) security message literature from premier IS and HCI-security publications; (2) IS-security research essays and calls for papers; and (3) NeuroIS literature. Approaches (1) and (2) helped identify important and relevant research questions, while approach (3) ascertained whether the research questions identified would be productively investigated using NeuroIS methods. This approach follows the recommendation of vom Brocke & Liang (2014), who emphasize the importance of selecting NeuroIS research questions that, first and foremost, answer problems of importance to the IS community, and second, benefit from studies using neurophysiological measures.

Survey of the IS and HCI-security literature

To identify articles describing security messages, we searched for articles in the AIS Senior Scholars basket of six journals (AIS-6; Lowry *et al*, 2013), and in premier computer science publications on human–computer interaction and security, including the Conference on Human Factors in Computing Systems (CHI), the Symposium on Usable Privacy and Security (SOUPS), and the USENIX Security Symposium. In each of these outlets, we searched for articles with security in the title, abstract, or keywords that were published before July 2014. We also filtered the articles based on whether they included terms derived from our taxonomy in Appendix A. We narrowed the articles to include only those that were behaviorally oriented and focused on security messages. Our review resulted in 29 articles, some of which addressed multiple research questions. These articles, combined with the IS search results, are listed in Table B1 of Appendix B.

Table 2 summarizes the overarching research questions extracted from the papers we reviewed and the count of articles that supported each one. Table B2 of Appendix B presents a detailed research question set showing each question identified and its frequency of occurrence. Several studies examined participants' attitudes, beliefs, and motivations related to security messages, but there was no cohesion on that topic. Thus, this article does not address this research question.

Table 1 Description and focus of measurement of commonly used neurophysiological tools

Neurophysiological tools	*Focus of measurement*	*Strengths*	*Weaknesses*
Psychophysiological tools			
Eye tracking (e.g., Proctor & Vu, 2006; Castellina *et al*, 2008)	Eye pupil location (gaze) and movement	Identify visual activity; clear visualization of what was viewed at any given moment	Does not capture peripheral vision; cannot ensure gaze equates with thought or attention; artificial setting may bias behavior
Skin conductance response (SCR) or electrodermal activity (EDA) (e.g., Dawson *et al*, 2011)	Sweat in eccrine glands of the palms or feet	Low cost; easy to use; minimal intervention on subjects	Lack of predictable measurement; habituation; still some debate on interpretation
Facial electromyography (fEMG) (e.g., Ekman *et al*, 1992; Minas *et al*, 2014)	Electrical impulses on the face caused by muscle fibers	High degree of precision, widely accessible, minimally invasive	Only a small number of muscles can be measured; difficulty with interpretation; setting may bias behavior
Electrocardiogram (ECG or EKG) (e.g., Ortiz de Guinea *et al*, 2013; Schellhammer *et al*, 2013)	Electrical activity on skin caused by heart muscles	Minimally invasive; low cost; widely accessible	Heart rate may be affected by a wide variety of factors
Measurement of cortisol levels (e.g., Wastell & Newman, 1993; Riedl, 2012)	Level of cortisol (commonly called the stress hormone) in one's bloodstream or saliva	Minimally invasive; low cost	Cortisol levels peak 10–40 min after stressor onset
Mouse-cursor tracking (e.g., Freeman & Ambady, 2010; Grimes *et al*, 2013)	The cursor location and movement properties on the screen	Inexpensive; non-invasive; mass-deployable; useful in natural and non-laboratory settings; surrogate for attention; changes in movement precision correlate with emotional changes	Cannot capture attention if the mouse cursor is not moving. Cannot ensure movement equates with thought or attention
Brain imaging tools			
Functional magnetic resonance imaging (fMRI) (e.g., Dimoka, 2010, 2012)	Blood flow changes or blood oxygenation level dependent signal (BOLD response) in the brain because of neural activity	Non-invasive; standard data analysis methods; spatial resolution	Artificial setting; temporal resolution (few seconds' delay); need to be careful with correlation *vs* causation
Positron emission tomography (PET) (e.g., Haier *et al*, 1988; Bench *et al*, 1993)	Metabolic changes in the brain because of neural activity	Spatial resolution	Invasive (because of injected tracer); potentially harmful; low temporal resolution (2–3 min)
Electroencephalography (EEG) (e.g., Minas *et al*, 2014; Vance *et al*, 2014)	Electrical potentials on the scalp because of neural activity	Inexpensive; tolerant of a little subject motion; directly measures electrical activity; temporal resolution in milliseconds	Spatial resolution; only sensitive to outer layers of cortex
Magnetoencephalography (MEG) (e.g., Pantev *et al*, 2004; Moses *et al*, 2007)	Magnetic field changes because of neural activity	Temporal resolution in milliseconds; deeper capability than EEG	Spatial resolution
Transcranial magnetic stimulation (TMS) (e.g., Hiraga *et al*, 2009; Schutter & van Honk, 2009)	Weak electrical current causes activity in specific parts of the brain – measure activity and function of specific connections/ pathways	Non-invasive; less expensive than fMRI	Can only stimulate 2 in deep; may induce seizure or fainting
Functional near-infrared spectroscopy (fNIR) (e.g., Kemper *et al*, 2007; Gefen *et al*, 2014)	Blood flow changes (BOLD response) in the brain because of neural activity	Non-invasive; less expensive and more portable than fMRI	Can only measure cortical activity 4 cm deep

Table 2 Reduced research questions sorted by article count

Research question	*Count*
Attention/habituation	22
Comprehension	18
Attitudes and beliefs, motivations	10
Fear	6
Dual-task interference	6
Stress	5
Gender differences	1
Social norms	1
Uncertainty	1

Table 3 Summary of rationale for selection of research questions

Research question	*Occurrence frequency (n)*	*Selected*	*Rationale*
Attention/ habituation	22	✓	Strong support
Comprehension	18	×	NeuroIS not necessary
Attitudes and beliefs, motivations	10	×	Items in this category too general, failed to coalesce around a central theme
Fear	6	✓	Strong support
Dual-task interference	6	✓	Strong support
Stress	5	✓	Strong support
Gender differences	1	×	No strong support in IS or CS literature
Social Norms	1	×	Frequency of occurrence too low
Uncertainty	1	×	Frequency of occurrence too low

Survey of the IS security calls for research

We next compared the research questions against (1) calls for papers (CFP) for special issues of journals and for conferences, and (2) IS security issues and opinion pieces. We performed this search by gathering papers from IS venues to determine whether any question from our reduced set of research questions in Table 2 should be weighted more heavily. The new set of papers consisted of 10 papers, listed in Table B3 of Appendix B.

In our analysis of these papers, Tarafdar *et al* (2013) strongly emphasized the need for stress to be researched. Similarly, Crossler *et al* (2013) explicitly highlighted the importance of fear in research. Many of the papers called for IS-security research on high-level topics such as 'behavioral security', 'explaining information security policy compliance', and 'volitional and accidental security policy violations'. Over half of the papers explicitly or implicitly called for research on the intention–behavior gap (discussed in the section 'Research agenda'). We found support for all of our research questions except for gender differences; thus, we removed it from our set of questions.

Survey of the NeuroIS literature

For the third step, we searched NeuroIS opinion publications and research agenda articles to evaluate whether the research questions identified above could be examined using neurophysiological measures. For this step, we collected all NeuroIS research agendas or opinion pieces published through 2014. This set included six articles, listed in Table B4 of Appendix B. On the basis of this review, all of the topics in Table 2 (omitting gender) could be considered 'antecedents of human behavior', which several articles suggest exploring with NeuroIS (e.g., Dimoka *et al*, 2011). Thus, we found support for studying each of the research questions using neurophysiological measures. Table B5 summarizes our NeuroIS paper findings.

Last, we evaluated whether conventional, non-NeuroIS methods would be better suited for studying our research questions. This follows Dimoka *et al*'s (2012, p. 694) guidance of having 'a good rationale for using neurophysiological tools'. We determined that while comprehension could be studied using NeuroIS methods, other methods such as talk-aloud protocols (e.g., Egelman *et al*, 2008; Felt *et al*, 2012), are also useful for examining comprehension. For this reason, we eliminated 'comprehension' from our set of research questions.

The above analysis led to the selection of four areas for our research agenda: (1) habituation, (2) fear, (3) stress, and (4) dual-task interference. Table 3 summarizes our rationale for the selection of these research questions. We excluded the remaining research questions for various reasons. Neither attitudes and beliefs nor motivations coalesced around a single theme, so we excluded those from consideration in this research agenda. Gender differences were not supported by IS security research essays and CFPs. The occurrence of references to uncertainty and norms in the information security literature was too low to be included in a different topic for this research agenda. Finally, we determined that comprehension is sufficiently examined using non-NeuroIS methods.

Research agenda

The four questions of this research agenda share the ability to explain the intention–behavior gap – the discrepancy between stated intentions and realized behaviors – a major problem of inquiry in the social sciences. In a meta-analysis examining the influence of intentions on behavior ($n = 82{,}107$ total participants), intentions accounted for 28% of variance in behavior, leaving 72% unexplained (Sheeran, 2002). This gap has special importance in the behavioral security domain because in securing systems, 'it is the behavior that matters and not the intention to perform the behavior' (Crossler *et al*, 2013, p. 95).

NeuroIS methods have great potential to measure cognitive and emotional factors that may strongly influence

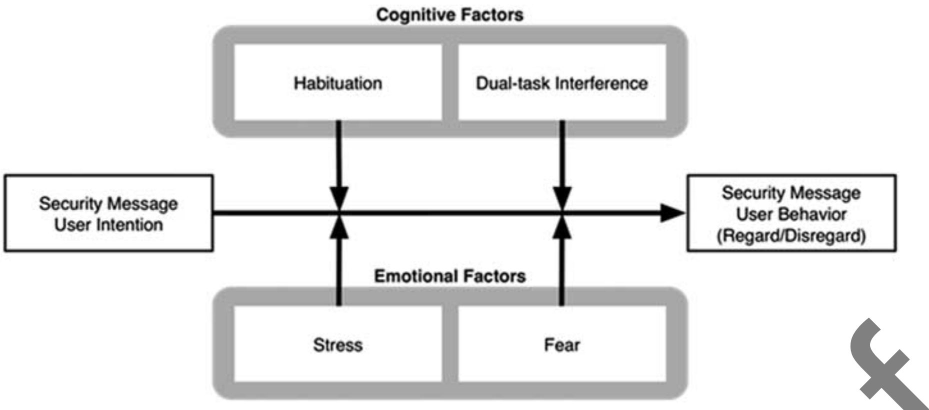


Figure 1 Framework for research questions.

behavior and yet not rise to the level of awareness (Riedl *et al*, 2014). For this reason, Crossler *et al* (2013) called for security scholars to employ NeuroIS methods to better understand factors influencing the intention–behavior gap. This point was empirically underscored by Vance *et al* (2014), who found that electroencephalography (EEG) predicted security behaviors substantially better than self-reported measures did.

Factors such as habituation, stress, fear, and dual-task interference help to explain behaviors that may appear to be careless, indifferent, or accidental security-related behavior (Vance *et al*, 2014). With this perspective, Figure 1 presents a framework that illustrates how each of the research questions, comprising cognitive and emotional factors, has the potential to moderate the relationship between users' intentions and behaviors in response to security messages. However, each of these factors may themselves exert direct effects on security behavior.

Research question 1: how does habituation affect users' responses to security messages?

A major contributor to security message failure is *habituation* – the diminishing of attention because of frequent exposure to warnings (Kalsher & Williams, 2006). Some laboratory experiments have pointed to the role of habituation in users' failure to heed warnings and security indicators (Good *et al*, 2005; Dhamija *et al*, 2006; Wu *et al*, 2006; Schechter *et al*, 2007; Sharek *et al*, 2008). Egelman *et al* (2008) found a significant correlation between recognition and disregard of security warnings. Sunshine *et al* (2009) observed that participants remembered their responses to previous security warnings and applied them to other Websites even if the level of risk had changed. Felt *et al* (2012) found that 42% of participants were not aware of having interacted with security permission dialogs before installing an Android app on their devices. Similarly, some participants in Sotirakopoulos *et al* (2011) study clicked through security warnings during a task, and later reported that they had not seen any security warnings (see also user account control prompts in Motiee *et al*, 2010).

These laboratory study results reflect those in the field. Akhawe & Felt (2013) found that in approximately 50% of the most common type of secure sockets layer (SSL) Web browser warnings in Google Chrome, users decided to click through in 1.7 s or less, a finding that 'is consistent with the theory of warning fatigue' (Akhawe & Felt, 2013, p. 14). Felt *et al* (2014) found that warning design explained between one-third and one-half of the difference between Chrome and Firefox SSL warnings. Bravo-Lillo *et al* (2013) conducted a large field experiment using Amazon Mechanical Turk in which users were rapidly exposed to a confirmation dialog message. After a period of 2.5 min and a median of 54 exposures to the dialog message, only 14% of the participants recognized a change in the content of the confirmation dialog in their control (status quo) condition.

Habituation: important gaps in the literature The literature reviewed above examined habituation indirectly by observing the influence of habituation on security behavior (Brustoloni & Villamarín-Salomón, 2007; Bravo-Lillo *et al*, 2013). For example, behavioral laboratory experiments, think-aloud protocols, interviews, self-report measures, and time-based measures have been used to identify whether stimuli capture attention or invoke mental processes related to habituation (e.g., Good *et al*, 2005; Egelman *et al*, 2008; Felt *et al*, 2012; Akhawe & Felt, 2013). While this research is valuable for demonstrating the existence of habituation, it does not directly measure the mental process of habituation, and therefore is unable to provide insight into (1) how habituation develops in the brain in response to security messages, and (2) how the neurological manifestation of habituation affects security behaviors. The lack of a means to directly measure these mental processes of habituation limits the ability to design security messages and interventions that directly address the phenomenon.

A fundamental gap in the above studies is that they examine habituation as a behavior, when in fact the phenomenon is neurobiological. Habituation, or repetition suppression as it is referred to in neuroscience, is one of the most pervasive and robust phenomena in neurobiology (Rankin *et al*, 2009). For example, Kandel and colleagues demonstrated in a series of now-classic studies using sea slugs that neural responses to a given stimulus decreased with repeated exposures to that stimulus (Kandel, 2001). This kind of repetition suppression to repeated stimuli has also been widely observed in humans (for review, see Grill-Spector *et al*, 2006). For example, using fMRI, researchers have observed involuntary decreases in mental activity (as measured via blood flow) for repeated stimuli at delays ranging from seconds to days (van Turennout *et al*, 2000). Studies that examine habituation without considering these neurological underpinnings provide only a partial view of the problem. Because habituation occurs unconsciously at the neurobiological level, interventions designed to encourage greater vigilance on the part of users – such as SETA programs – will have limited efficacy.

It should be noted that despite sharing the same Latin root, the construct of habituation is very different from the construct of habit. Habit is defined as 'learned sequences of acts that have become automatic responses to specific cues, and are functional in obtaining certain goals or end-states' (Verplanken & Aarts, 1999, p. 104). Thus, habit occurs at the behavioral level, and involves learned behaviors that are associated with specific outcomes. In contrast, habituation occurs at the neurobiological level (Ramaswami, 2014), and does not require subsequent behavior, but occurs involuntarily without conscious awareness (Grill-Spector *et al*, 2006).

Another important gap in the habituation literature is that current approaches do not reveal how perception changes over time. The EMM effect explains that people begin 'seeing' a familiar stimulus less via visual scrutiny and more from memory of their first view of the stimulus (Smith *et al*, 2006). This phenomenon is manifested systematically in fewer eye-gaze fixations and less visual sampling of regions of the image after repeated viewings (Hannula *et al*, 2010). In this way, eye movement is an index of a person's attention to and memory of an image over time (Beck *et al*, 2007; Hannula & Ranganath, 2009). This is an important aspect of habituation that traditional measures do not capture, and has important implications for the display of security messages. It suggests that security messages should highlight differences in warnings or their appearance should change, rather than relying on users to visually scrutinize the warnings.

Habituation: how NeuroIS can be used to address these gaps NeuroIS can help address the above gaps by directly measuring the mental process of habituation to determine (1) how quickly habituation develops in response to security messages, (2) how the neurological manifestation of habituation affects security behaviors, and (3) how long the effects of habituation on security messages persist. NeuroIS measures of habituation could potentially enable the testing of security messages and interventions that are resistant to habituation, minimize its effects, and speed recovery from habituation to security messages.

Of the various NeuroIS methods, fMRI and eye tracking are especially relevant when studying habituation. fMRI can track neural activation through changes in blood oxygenation, known as the blood oxygenation-level-dependent (BOLD) response. fMRI can determine whether there is a decrease in activation (the repetition suppression effect) in brain regions associated with visual processing when security warnings are viewed repeatedly. The repetition suppression effect has been established in the context of images (e.g., Bakker *et al*, 2008), but it is not yet clear how this effect applies to security messages that have both visual and textual elements.

Eye tracking is an appropriate tool to measure habituation. Eye-tracking tools can precisely measure eye position and movement (Shimojo *et al*, 2003), including eye fixation, pupil dilation, and gaze duration on areas of interest (Rayner, 1998). Distinct from other NeuroIS tools, eye tracking's most notable advantage is its ability to measure human visual activities with a high level of accuracy and temporal precision. This information is not possible through self-reporting because people are unable to perfectly recall or not fully conscious of what they saw, where they looked, and in what order they looked (e.g., Schechter *et al*, 2007; Egelman *et al*, 2008; Sunshine *et al*, 2009). Eye tracking allows researchers to understand what participants attend to, and therefore what can be perceived (Smith *et al*, 2006; Benbasat *et al*, 2010). Eye-tracking tools provide data such as heat maps to indicate the percentage of time spent gazing at any particular area. Therefore, capturing the EMM effect through an eye tracker is a robust means of evaluating habituation.

A possible experimental design for using either fMRI or eye tracking to study habituation is a within-subject, repeated measures laboratory experiment. Images for a variety of security messages could be repeatedly displayed to participants. To measure habituation's onset, the BOLD response level for fMRI, the number of eye-gaze fixations, or length of gaze duration could be compared across the first, second, and subsequent exposures for each image of a security message. Because time is inherent to the process of habituation, the above approach could be extended to a longitudinal design to gauge how habituation to security messages changes over days (with experimental sessions at the same time every day) or over weeks (with experimental sessions once a week for several weeks).

Research question 2: what is the impact of stress on a user's response to security messages?

Recent research has highlighted the importance of examining 'technostress' (e.g., Tarafdar *et al*, 2013), which is stress caused by interactions with information communication technologies (Brod, 1984). Stress can have profound detrimental effects on individuals' productivity and well-being (Riedl, 2012). One perspective of stress is as an evaluative transaction between an individual and a required task when the individual perceives that he or she lacks the resources or skills necessary to complete a required task (Cooper *et al*, 2001; Ayyagari *et al*, 2011).

Being under stress affects an individual's physiology, affect, and behavior (Sonnentag & Frese, 2003). An individual under chronic stress is more likely to have narrowed attention and poorer working memory capacity (Searle *et al*, 1999). These outcomes of stress on behavior have been associated with individuals making poor decisions; for example, Wall Street traders under stress made worse risk evaluations than traders did under less stress (Riedl, 2012). Intrusive technology characteristics are a strong predictor of stressors for users, and work overload is one of the most prevalent stressors (Ayyagari *et al*, 2011). Perceiving system annoyances often results in heightened stress states (Riedl, 2012).

D'Arcy *et al* (2014) showed that technostress has important implications for end-user security. They conceptualize 'security-related stress' (SRS) as comprising the subdimensions of work overload, complexity, and uncertainty of security requirements. In a field survey, they found that SRS significantly influenced moral disengagement, and indirectly, intention to violate information security policy. Several studies have sought to avoid or diminish technostress-related problems in connection with users experiencing security messages. Felt *et al* (2012) recommended a more parsimonious set of Android permission prompts to avoid overwhelming users with too much information. Dhamija & Tygar (2005, p. 4) emphasized that their security tool '[placed] a very low burden on the user in terms of effort, memory and time'. Akhawe & Felt (2013) reasoned that a high level of browser SSL warning click-through rates might be the users' annoyance with too many warnings. Security in general can be stressful for users – in a study of password meters, participants reported annoyance with meters that had stringent security demands (Ur *et al*, 2012). Given these pernicious outcomes of stress on security message interactions, it is important to better understand the role of stress in users' security decisions.

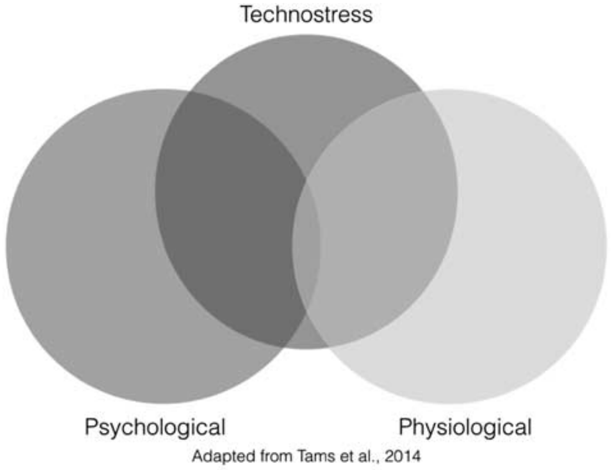
Stress: important gaps in the literature The work of D'Arcy *et al* (2014) illustrates an important gap in the stress-related security literature: self-report measures capture only one aspect of the technostress – the perceptual measure of stress-inducing conditions. D'Arcy *et al* (2014, p. 308) consider this as a limitation of their and 'most psychological stress research' and call for future research to 'build on our initial work and utilize objective measures (e.g., physiological techniques) to gauge SRS'. This gap is highlighted by Tams *et al* (2014) who conducted a study to compare the ability of self-report and physiological measures to capture the construct of technostress. They found that salivary α-amylase explained variance in performance of a computer-based task beyond that predicted by self-report stress measures. They explained that:

> Physiological measures are complements to psychological ones rather than alternatives; the triangulation of physiological measures with psychological ones can result in a more holistic representation of IS constructs. This finding suggests that physiological measures are a vital complement to existing methods since they can improve the prediction of outcomes related to such IS phenomena as technostress above and beyond that afforded by psychological measures. (p. 737)

Tams *et al* found that the physiological and self-report measures of technostress did not correlate. They therefore concluded, consistent with the technostress and neurobiological literature, that their self-report and physiological measures of technostress corresponded to the conscious and unconscious aspects of technostress, respectively (see Figure 2).

These findings have important implications in the context of security messages, in which users are not always aware of their emotions (Dimoka *et al*, 2011; Lopatovska & Arapakis, 2011). Because security messages often appear for only a short duration and frequently lack users' full attention, users may have difficulty accurately recalling and reporting their level of stress while viewing the message. Hence, users' self-reported emotions are often inconsistent with their actual emotions (Tams *et al*, 2014), and measures of stress alone are likely to be insufficient (Riedl, 2012), leading to an incomplete understanding of how technostress affects the processing of security messages and partial solutions for security practice. Tams *et al* (2014) suggest a combination of psychological and physiological measures to fully capture the construct of technostress.

NeuroIS methods can provide several insights into the relationship between the processing of security messages



Adapted from Tams et al., 2014

Figure 2 How psychological and physiological measures capture different aspects of the technostress construct.

and stress that would otherwise be difficult to obtain. For example, NeuroIS can explore how actual physiological stress (rather than self-reported stress) influences the reception of security messages (Tams *et al*, 2014). NeuroIS tools can be used to measure the magnitude and duration of stress and its influence on security message disregard and performance, which may be subject to biases, recall error, and unawareness if measured using self-reporting for discrete events such as interactions with security messages (Tams *et al*, 2014). NeuroIS tools can explore which neurological functions are inhibited by stress, and at what levels they are inhibited (Riedl, 2012). Researchers can thereby design security messages that are less reliant on these neurological functions, and can be processed more effectively under stressful conditions. In each of these scenarios, NeuroIS offers the potential to provide new insights into how technostress influences users' reactions to security messages that would be difficult to obtain otherwise.

Stress: how NeuroIS can be used to address these gaps Two neurophysiological methods for measuring stress are cortisol-level measurement and skin conductance response (SCR). Cortisol is commonly called the stress hormone. Cortisol and other biological measurements are often favored because they can measure unconscious stress responses (Riedl, 2012; Riedl *et al*, 2012). When an individual's stress level increases, so does the amount of cortisol in the body as psychological stressors stimulate its release into the bloodstream. Cortisol mediates stress responses and returns the body to homeostasis (Dickerson & Kemeny, 2004). Cortisol levels peak 10–40 min after stressor onset as measured using blood, spinal fluid, or saliva samples (Dickerson & Kemeny, 2004). Riedl *et al* (2012) demonstrated how technostress could be measured using cortisol samples. Examining cortisol levels allows researchers to objectively measure stress associated with security messages.

SCR is also known as galvanic skin response or electrodermal activity. The increase in the activity of sweat glands when an individual is stressed creates a temporary condition in which the skin becomes a better electricity conductor (Randolph *et al*, 2005). SCR has been linked to measures of arousal, excitement, fear, emotion, and attention (Raskin, 1973). SCR tools can measure activity in the sympathetic nervous system that changes the sweat levels in the eccrine glands of the palms. SCR is inexpensive which makes it widely accessible. In addition, SCR is relatively easy to use and requires minimal intervention on subjects (Dimoka *et al*, 2012). We believe that SCR will be useful in measuring the stress levels associated with users' responses to security messages.

An experimental design to test technostress would include a set of treatments wherein participants would react to computer security messages. The researchers could collect saliva samples before and after the tasks and compare the levels of cortisol across the treatments. One would expect the level of cortisol to increase for each participant because of the nature of the study. In particular, participants who were engaged in the most stress-inducing condition would be likely to have the highest levels of cortisol in the post-experiment assessment.

Research question 3: how does fear influence our neural processing of security messages?

Fear can have a powerful impact on how individuals respond to security messages. Fear is an emotional state that occurs in response to the presence of a threat to safety (Witte, 1992; Whalen, 1998). It prompts threat-withdrawal (Frijda, 1986) or safety-approaching behaviors (Blanchard & Blanchard, 1994). In an information security context, both benevolent and malicious messages commonly attempt to elicit fear to motivate the target into action.

Benevolent security messages such as fear appeals describe a threat to an individual, and aim to invoke fear as a means of motivating the recipient toward protective security behaviors (Johnston & Warkentin, 2010; Johnston *et al*, 2015). Johnston & Warkentin (2010) found that fear appeals lead to higher intentions to install anti-spyware than non-fear appeal messages did. In Vaniea *et al* (2014) study of user reactions to application update requests, some participants reported trepidation fueled by past negative experiences about the unknown consequences of an update on their computer or workflow. Similarly, Good *et al* (2005) observed participants' interactions with EULAs as they installed software on their personal computers, and categorized many users as being 'once bitten, twice shy' or 'computer-phobic', meaning moderately or extremely afraid of adverse consequences that could result from installing the software. In a study evaluating user interactions with password strength meters, Ur *et al* (2012) found that some participants stated that they were afraid of the consequences of having a weak password. Field studies have found similar results for fear and security messages. Felt *et al* (2014) found that SSL warnings with an image of a criminal were associated with significantly lower click-through rates than were warnings with images of police officers or red stoplights. The authors reasoned that fear may be the factor explaining this difference.

Malevolent security messages often describe an artificial threat to evoke fear to goad a user into action. For example, phishing messages may contain ominous warnings about a threat to a user's bank account if the user does not immediately verify their login credentials (Drake *et al*, 2004; Kessem, 2012). While users may know about the existence of phishing schemes, strong emotions such as fear may invoke automatic responses that bypass cognition (Ortiz de Guinea & Markus, 2009), leading an individual to fall victim to the attack. Such tactics take advantage of human tendencies to be more risk averse and risk pessimistic while experiencing fear (Lerner & Keltner, 2001); for example, complying with a phishing e-mail and supplying account credentials may seem to be the conservative risk option in that it supposedly prevents the closure of an account and loss of funds.

Fear: important gaps in the literature Although fear-related models, such as protection motivation theory (PMT), are one of the most dominant theoretical perspectives in behavioral information security research, the construct of fear has rarely been directly measured (Boss *et al*, 2015). Vance *et al* (2012) used a survey to measure PMT-related constructs such as perceived threat vulnerability and threat severity, but threat and fear are different constructs (Boss *et al*, 2015). Fear has been shown to be an important mediator of the threat appraisal process (Rogers & Prentice-Dunn, 1997; Floyd *et al*, 2000). The absence of fear measurement in PMT-related studies such as that of Vance *et al* (2012) therefore constitutes a missed opportunity that could have altered reported findings.

Several calls have been made for using NeuroIS methods to more effectively measure fear in an information systems context (e.g., Dimoka *et al*, 2011; Dimoka *et al*, 2012; Crossler *et al*, 2013; vom Brocke & Liang, 2014). For example, Boss *et al* (2015) explain:

> … the ideal fear measure might be one that is applied at the moment of occurrence. This is best achieved under tight experimental controls (e.g., fMRI, EKG, or galvanic skin response). Creating a realistic fear measurement of ISec behaviors under such conditions is thus highly complex and could be the "holy grail" of this line of research … It might be necessary to use slightly less invasive techniques, such as eye tracking (e.g., Twyman *et al*, 2015), examining mouse movements (e.g., Hibbeln *et al*, 2014), recording keystroke delay (e.g., Jenkins *et al*, 2013), or leveraging a wearable galvanic skin response measurement device (e.g., Moody & Galletta, 2015).

Self-report measures of fear are susceptible to social desirability bias, subjectivity bias, common method bias, and people's awareness of their emotion (Dimoka *et al*, 2011; Lopatovska & Arapakis, 2011). NeuroIS can help mitigate these challenges by objectively measuring fear as it occurs.

Another gap in existing studies that Vance *et al* (2012) illustrated is the underlying assumption that individuals perceive as personally relevant threats to data and systems. Johnston *et al* (2015) explain that 'to appeal to the self-interests of their audience, fear appeals must achieve a sufficient level of personal relevance (or issue involvement) for the individual; otherwise, they are ignored and rendered ineffective' (p. 114). Although PMT assumes that all threats are personally relevant, it is not clear whether individuals perceive threats to their personal data and systems the same way. This discrepancy is even greater for studies such as Vance *et al* (2012) that use organizational data because the information and systems under threat typically do not belong to the individual, but rather to the individual's employer. Johnston *et al* (2015):

> The dominant logic behind the application of fear appeals and PMT to information security phenomena was that threats to data, information, systems, and so on would be regarded in the same manner as threats to one's personal safety or health and have universal, personal relevance. We challenge this flawed logic. PMT does not account for the distinction in the nature of the espoused threat and, therefore, has been repeatedly misspecified in the security literature.

Thus, a gap in the fear-related security literature is whether perceptions of threats to one's data, information, and systems differ Warkentin *et al*. (forthcoming) examine this issue in the context of fear appeals. They found that reading information security fear appeals did not activate the amygdala. The authors suggest that this may have been because of low personal relevance of the information threat. More research is needed to determine whether other types of security messages elicit fear. Also, future research can investigate whether fear appeals can be designed to foster emotive fear through highlighting more personally relevant consequences of information threats, such as increased stress and worry from perceptions of threats to one's person, and whether threats to external information assets are considered personally relevant when they belong to another entity. These two types of perceived threats may represent entirely different constructs. NeuroIS has been proven to be useful in disentangling related IS constructs (Dimoka, 2010). As Dimoka *et al* (2012) highlights, 'the localization of the neural correlates of IS constructs with neuroimaging data can shed light on their nature, conceptualization, and dimensionality' (p. 692).

A third gap is that studies like Vance *et al* (2012) only entail a cognitive threat assessment, whereas visceral emotion is an important characteristic of fear (Dimoka *et al*, 2011). This gap has been noted by Crossler *et al* (2013):

> Behavioral InfoSec research that captures perceptions of fear does so via a survey methodology or embedded within a lab experiment. For InfoSec 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. … In the studies to date, subjects cognitively assess the instrument items and their perceptions in cognitive terms, not in the moment of fear occurrence, but rather as a self-assessment of a perspective determined post-stimulus … Future research could further utilize fMRI, EEG, or other physiological techniques in a laboratory setting to better capture the extent to which fear is realized in its affective (emotional) and then cognitive forms.

Because the experience of emotion is a key aspect of fear, the existing fear-related literature is incomplete. Further, emotions are difficult to measure using traditional survey methods because they often do not rise to the level of awareness (Riedl *et al*, 2014). This suggests the need for NeuroIS methods to measure the emotional aspect of fear and how it affects the reception of security messages.

Fear: how NeuroIS can be used to address these gaps Fear has been captured in neuroscience studies with fMRI (Hsu *et al*, 2005; Krain *et al*, 2006) and associated with activity in the amygdala, the orbitofrontal cortex, and the striatum (see also Platt & Huettel, 2008; Sarinopoulos *et al*, 2010). We propose that facial electromyography (fEMG) is a useful psychophysiological tool to detect fear in subjects performing a computing task such as interacting with security messages. With fEMG, visually imperceptible EMG activity in the muscle regions associated with facial expressions (over the brow – corrugator supercilia, eye – orbicularis oculi, and cheek – zygomatic major) can differentiate the intensity and valence of an individual's reactions to visual stimuli. Cacioppo *et al* (1988) found that 'EMG activity over the muscles of facial expression can provide objective and continuous probes of affective processes that are too subtle or fleeting to evoke expressions observable under normal conditions of social interaction' (p. 260). More recently, Minas *et al* (2014) used fEMG to examine activity in the corrugator supercilia to determine the emotional responses in a virtual team setting.

In addition to the brain-imaging tools (see Table 1), one could use mouse-cursor tracking to study fear. When experiencing fear, people have a lower ability to control their attention on a single stimulus or destination – that is, people uncontrollably allocate their attention more broadly to increase awareness of possible threats (Eysenck *et al*, 2007). Shifts in attention are measured through the analysis of mouse-cursor movements (e.g., Chen *et al*, 2001; Guo & Agichtein, 2010), as hand movements are biased toward stimuli that, even briefly, capture a person's attention (Welsh & Elliott, 2004). As people allocate attention more broadly to stimuli when experiencing fear, the hand deviates away from the intended trajectory (in the directions of these stimuli), resulting in less precise movements (e.g., Grimes *et al*, 2013). These deviations can be measured through analysis of the cursor's movement trajectory (see Hehman *et al*, 2014 for example analyses).

Potential experimental designs using fMRI or fEMG could display the elements of fear appeals that describe specific threats and then measure whether and how fear is elicited. Similarly, elements of fear appeals linked to coping responses could be displayed to determine which neural correlates relate to the coping response process. These neurophysiological measures could then be compared with self-reported measures of threat and coping appraisals, and to reported behavioral intention. Mouse cursor tracking could be useful to unobtrusively measure responses to fear appeals as they are encountered during naturalistic tasks. This objective behavioral data could be used to evaluate the effectiveness of different fear appeal design treatments.

Research question 4: how does dual-task interference disrupt cognitive processing of security messages?

Dual-task interference is a neurological phenomenon that explains why people have trouble performing two or more relatively simple tasks concurrently (Pashler, 1994). Dual-task interference can influence how people perceive and cognitively process security messages, and may be particularly useful for understanding users' responses, because people respond to security messages while performing other primary tasks on a computer, such as completing a work-related task, searching the Internet, or using the computer for entertainment (West, 2008). As such, when a security message prompts a user's attention, a person's working memory and cognitive functions may be deployed in the primary task. In this scenario, the message must compete for these cognitive resources, and thus one's response to the message is subject to dual-task interference (Pashler, 1994).

Normally, people are not aware of tasks interfering with each other (e.g., responding to a security message while completing another task on the computer) unless the two tasks are cognitively difficult, physically incompatible, or evoke negative emotional reactions; thus, responding to security messages while using the computer for other low cognitively demanding tasks might seem immune to dual-task interference. However, studies demonstrate that the opposite is true: tasks can 'interfere with each other quite drastically, even though they are neither intellectually challenging nor physically incompatible' (Pashler, 1994, p. 220). For example, when people are involved in even simple cognitive tasks, they cannot process information or perform behaviors related to other tasks as quickly or effectively (e.g., Logan, 1978; Kleiss & Lane, 1986; Duncan & Coltheart, 1987). From a neurological perspective, research has found that this dual-task interference may result from tasks competing for the same brain functions (Rémy *et al*, 2010), and is enhanced when performing two or more tasks while experiencing stress (Plessow *et al*, 2012).

Dual-task interference has been suggested as a primary reason for users' neglect of security behaviors (Jenkins & Durcikova, 2013). Yee (2004) suggests that 'interrupting users with prompts presents security decisions in a terrible context: it teaches users that security issues obstruct their main task and trains them to dismiss prompts quickly and carelessly' (p. 49). Users may choose to dismiss warnings quickly and carelessly in this context because it is cognitively difficult for them to switch between their primary task and optimally address the security warning. Bravo-Lillo *et al* (2011) suggest that interrupting prompts are often ignored or suboptimally addressed because users have a limited cognitive ability to switch between tasks. Felt *et al* (2012) found that the vast majority of people do not pay attention to nor comprehend permission warnings, and nearly half of laboratory study participants are completely unaware of permission warnings. These findings suggest that cognitive functions associated with awareness and comprehension may be limited in the presence of dual-task interference. Furthermore, when browsing the Internet, people pervasively ignore and quickly dismiss security warnings that pop up in the middle of another task (e.g., Akhawe & Felt, 2013). Although many factors contribute to the automatic dismissal of security warnings, one potential explanation is that people have difficulty devoting the necessary cognitive resources to process the warning while performing other tasks.

Dual-task interference: important gaps in the literature The literature has reported the behavioral effects of dual-task interference, but has not yet explored its neurological underpinnings. Research suggests three competing models that may explain how dual-task interference influences users' responses to security messages: (1) the capacity-sharing model, (2) the bottleneck (task-switching) model, and (3) the cross-talk model (Jenkins & Durcikova, 2013). The capacity-sharing model explains that when people perform multiple tasks together, less cognition is available for each task, as the tasks share limited cognitive capacity (Tombu & Jolicœur, 2003). The bottleneck model suggests that if one task is using a cognitive resource, it is not available for other tasks (Pashler, 1994; Dux *et al*, 2006; Sigman & Dehaene, 2006). The cross-talk model suggests that concurrent tasks cause the mind to confuse the various sources of information, resulting in biases and reduced performance (Koch, 2009). These neurological effects of dual-task interference on security message disregard can only be directly observed using NeuroIS methodologies.

Understanding the neurological underpinnings of dual-task interference is an important gap to address because it validates dual-task interference as an appropriate theoretical approach. Although behavioral studies have used dual-task interference as a theoretical lens to explain security message disregard (e.g., Jenkins & Durcikova, 2013), they have not established that dual-task interference exists when people respond to security messages. It is therefore unclear whether dual-task interference is the primary cause of the observed effects, or if other factors are at work. A neurological understanding of dual-task interference could also guide the design and development of more effective security warnings. A security message should be designed differently depending on whether the capacity-sharing model, the bottleneck model, or the cross-talk model best accounts for security message disregard. For example, if NeuroIS tools indicate that the brain shares cognitive resources among concurrent tasks while responding to security messages (the capacity-sharing model), an effective security message design could guide the user through the decision-making process to rely less on shared resources. If the primary task inhibits people from activating brain functions needed to properly respond to security messages (the bottleneck model), security messages could be designed to temporarily stop the primary task so that these resources will be available (i.e., allowing the user to cognitively offload the primary task). If NeuroIS tools indicate that information from other tasks is biasing one's response to the security message (the cross-talk model), security messages could be accompanied by other cues (colors, sound, and images) to prime thoughts that promote positive cross-talk (e.g., enhancing perceived threat).

Another gap that NeuroIS can help address is to identify which regions of the brain are influenced by dual-task interference while people are responding to security messages. This gap has not yet been addressed in the behavioral approach of past studies (e.g., Jenkins & Durcikova, 2013), but it is important to address for more effective security message design. For example, if NeuroIS tools indicate that dual-task interference occurs in the medial temporal lobe of the brain (the area responsible for declarative or long-term memory), warnings could be designed to be less reliant on memory by providing just-in-time reminders and other relevant information that would otherwise be stored in long-term memory.

Dual-task interference: how NeuroIS can be used to address these gaps Brain imaging methodologies (see Table 1) are effective in measuring dual-task interference, and several studies have used fMRI (e.g., Herath *et al*, 2001; Szameitat *et al*, 2002; Jiang, 2004). EEG can be an effective technique for examining the cognitive consequences of dual-task interference. Using EEG, the P300 brainwave component of the event-related potential can be examined, which is associated with attention and memory operations (Polich, 2007). The P300 reflects brain activity approximately 300–600 ms after exposure to a stimulus. The speed of this measure reveals reaction differences in subjects before they have time to consciously contemplate a response. Monitoring a person's EEG measures as they perform a computing task that a security message interrupts can allow researchers to see the degree to which the message disrupted the task and the level of cognitive resources devoted to the message. Vance *et al* (2014) used EEG to predict user behavior in response to security warnings.

Another brain-imaging tool that could be useful for studying dual-task interference is functional near infrared spectroscopy (fNIR). fNIR uses certain wavelengths of light to measure changes in oxygenated and deoxygenated hemoglobin (BOLD response) and it is especially effective in brain regions close to the scalp, such as the frontal cortex (Cui *et al*, 2011). McKendrick *et al* (2014) used fNIR to monitor subjects performing a dual verbal-spatial working memory task and observed changes in activity in the dorsolateral prefrontal cortex (DLPFC) during the experiment. Gefen *et al* (2014) demonstrated the applicability of fNIR to enhance research in information systems, specifically in research related to multitasking. The ease of use and low costs associated with fNIR make it a prime candidate for NeuroIS research on security messages.

Potential experimental designs could use fMRI, EEG, and fNIR to measure the influence of dual-task interference on security messages in a within-subject design in which each participant would respond to security messages in three scenarios: (a) during a high dual-task inference time, (b) during a low dual-task interference time, and (c) during a no dual-task interference time. A simple way to induce high dual-task interference is to have participants memorize a seven-digit alphanumeric code, respond to a security message, and then recall the code. Requiring users to maintain the code in working memory while responding to the security message induces high dual-task interference. A low dual-task interference time can be between completed tasks: having a person memorize a code, recall the code, and then respond to a security message. A no dual-task interference time can be a scenario in which participants' only task is to respond to security messages. By comparing brain activation for the high dual-task interference, low dual-task interference, and no dual-task interference times, researchers can assess the impact of dual-task interference on the neural processing of security messages, and test whether some security messages are more robust to dual-task interference than other messages.

Empirical example

This section describes an experiment as an example of how to use NeuroIS to pursue one of the research questions, habituation to security messages. It is an illustrative example rather than a substantial knowledge contribution in its own right, but the experiment shows the value of using NeuroIS to investigate the research questions.

As noted in the section 'Habituation: important gaps in the literature', a gap in our understanding exists for how habituation to security messages occurs in the brain because habituation is difficult to measure directly with conventional methods. Anderson *et al* (2015) took an initial step to address this gap by using fMRI to show how habituation develops in the brain. Using the BOLD effect, the researchers were able to measure changes in blood flow to different brain regions, which in turn is indicative of localized brain activity (Anderson *et al*, 2015). Their results showed a dramatic drop in the visual processing centers of the brain after the second exposure to a warning, with further decreases upon subsequent exposures. The researchers designed warnings whose appearance is updated with each exposure (i.e., polymorphic warnings) to manipulate habituation. Their fMRI results demonstrated that the polymorphic warnings were significantly more resistant to the development of habituation in the brain than conventional warnings were.

Although the Anderson *et al* (2015) results represent a promising first step to examine the problem of habituation using NeuroIS methods, Dimoka *et al* (2012) emphasize that 'no single neurophysiological measure is usually sufficient on its own, and it is advisable to use many data sources to triangulate across measures' (p. 694). Accordingly, in the following example, we use (1) a different NeuroIS method, eye tracking; and (2) a different neurological phenomenon, the EMM effect, to triangulate the fMRI results of Anderson *et al* (2015). Whereas fMRI has superior spatial resolution for identifying which parts of the brain are influenced by habituation, eye tracking has superior temporal resolution for understanding the progressive occurrence of habituation. Utilizing the strengths of both methods, we can validate these methods' ability to measure the phenomenon of interest (Dimoka *et al*, 2012), in this case habituation.

Eye tracking and hypotheses

Eye tracking is a NeuroIS method (Dimoka *et al*, 2012) that is well suited for measuring habituation in our study for three reasons. First, eye tracking, like many other NeuroIS methods, excels at capturing 'hidden (automatic or unconscious) mental processes (e.g., ethics, deep emotions) that are difficult or even impossible to measure with existing measurement methods and tools' (Dimoka *et al*, 2011, p. 688). Habituation is one such process because it is automatic and fundamentally occurs at the neurological level (Grill-Spector *et al*, 2006); people are likely not fully aware of the extent of their habituation to warnings. In the study's context, eye tracking can capture the neurological EMM effect, and therefore directly measure habituation to security messages. Second, security warnings are visual stimuli that require attention to the details of their appearance and message. Eye tracking can fully capture users' visual inspection of warnings. Third, habituation and decisions to respond to warnings occur very quickly (Bravo-Lillo *et al*, 2013). With temporal precision in the tens of milliseconds, eye tracking is well suited to examine habituation to visual stimuli.

Per the EMM effect (see the section 'Habituation: important gaps in the literature'), we hypothesize that over repeated views of security warnings, people will exhibit fewer eye-gaze fixations and less visual sampling of the warning (Smith *et al*, 2006). Many warning styles follow similar design principles; for instance, indicators of alarm include bright red colors, exclamation marks, bold text, and two buttons for choosing whether to heed or ignore the warning. As users are exposed to repeated warnings, they will become more familiar with their common design, even if they originate from different applications. This increased familiarity should lead to increased reliance on memory, which should in turn be associated with decreased visual processing, according to the EMM effect. Accordingly, we hypothesize:

H1: Warning gaze duration will decrease over successive viewings per subject.

However, constantly changing the visual appearance of a warning type (i.e., a polymorphic warning) should prevent users from becoming habituated to the warning as quickly. Memory will be relied on less because the warning's appearance will be different from the last time it was viewed, so there will not be a perfect match between the modified polymorphic warning and an existing memory. Consequently, users will be more likely to give higher visual attention to a polymorphic warning over repeated viewings as opposed to a statically presented one. In summary, we hypothesize:

H2: Warning gaze duration will decrease more rapidly when viewing static warnings compared to polymorphic warnings.

Methodology

To test our hypotheses, we implemented a within-subject design in which people randomly viewed variations of polymorphic or static warnings. We then explored the number of fixations people made on the entire warning and the warning text over subsequent viewings to gauge the EEM effect.

We first developed a polymorphic warning UI-design artifact. To do so, we used the warning science literature to develop nine graphical variations of a warning dialog expected to capture attention. Our polymorphic warning artifact rotated through the graphical variations on each subsequent exposure. Each graphic variation was chosen based on variation suggestions in the literature. Table 4 lists each variation with its supporting sources, and Figure 3 depicts each variation for one example warning.

Experimental design

We used a Tobii T120 (see Figure 4) to measure the EEM effect. The eye tracker can track participants' eye movement with or without corrected vision (contact lenses and glasses), so we did not need to exclude any participants based on eyesight.

Participants were instructed to sit in a chair in front of the desk where the Tobii monitor was stationed. Using the Tobii software, participants' seating was adjusted until their gaze was in the optimal range. Participants also had their eye tracking calibrated with a task that had a moving red dot (slightly increasing and decreasing in size throughout the calibration) that would move around the screen. In this way, we could determine, based on output from the system, whether all the regions of the screen were sufficiently tracked. If there was an error, the participant was resituated and recalibrated. The calibration process took approximately 5 min.

Participants were then presented with a series of warnings. Each participant saw 10 warnings: five randomly assigned to the polymorphic treatment and five to the static treatment. Each warning was repeated 10 times. For the polymorphic warning, participants saw the nine variations plus the original image. For the static treatment, participants saw the same warning repeated 10 times. The images were randomly selected and displayed using the sequencing feature of the software. The experiment lasted from 10 to 20 min.

Participants were instructed to examine each warning carefully (see Figure 3) and assess whether the warning was: (1) novel within the study context, (2) similar to or a modified version of a previous image, and (3) identical to other images within the study. The warnings were self-paced, meaning participants could control how long they viewed each image before proceeding. This was done to mimic real life in which people choose how long to view a warning before dismissing it.

After viewing all of the warnings, we administered a post-experiment survey with demographic information, security attitude, and behavior intentions. To ensure manipulation validity (Straub *et al*, 2004), the post-test survey included a manipulation-check question that displayed a polymorphic warning as it rotated through its variations. Participants were asked if they noticed the treatment during the task. All but five of the participants reported that they had noticed the experimental treatment, which indicated successful overall manipulation. Following Straub *et al* (2004), we elected to retain participants who reported that they were not manipulated to provide 'a more robust testing of the hypotheses' (p. 408).

Participants

We pilot tested our experimental design with 20 participants. After making adjustments, we ran the final version of the experiment and collected usable data from 62 participants. Students were recruited from a large private university in the United States and given extra credit for participating. Participant age ranged from 18 to 30 with a mean of 21.66 years. Of the 62 participants, 23 (37%) were female. Each participant saw approximately 110 warnings, resulting in 6200 observations.

Analysis

The hypotheses were analyzed using latent growth curve modeling, a longitudinal statistical technique used to estimate growth trajectories over time (McArdle & Nesselroade, 2003). The analysis estimates an intercept and slope for observed values over time. In the study context, the observed values refer to the number of fixations on the warning and the text across each successive viewing of a warning.

Our eye tracker recorded fixations at a rate of 60 hz, capturing millions of eye movement records from participants as they viewed the warnings. The number of

Table 4 Polymorphic variations and their support from the literature

	Support
Text Appearance	
Color of text (red text)	Laughery *et al* (1993), Braun *et al* (1994)
Highlighting of text (yellow highlighting)	Strawbridge (1986), Young & Wogalter (1990)
Message Content	
Pictorial symbols (an exclamation point)	Kalsher *et al* (1996), Sojourner & Wogalter (1997)
Signal word ('Attention')	Silver & Wogalter (1989), Kalsher *et al* (1995)
Warning Appearance	
Color (red background)	Braun & Silver (1995), Rudin-Brown *et al* (2004)
Contrast (white on black)	Sanders & McCormick (1987), Young (1991)
Ordering of options (reordered)	Brustoloni & Villamarín-Salomón (2007), De Keukelaere *et al* (2009)
Size (large)	Vigilante & Wogalter (2003), Wogalter & Vigilante (2006)

Add "Forecast (Extension)"?

It can:

- Access all data on your computer and the websites you visit
- Access your data on all websites
- Detect your physical location

Add "Forecast (Extension)"?

It can:

- Access all data on your computer and the websites you visit
- Access your data on all websites
- Detect your physical location

Add "Forecast (Extension)"?

It can:

- Access all data on your computer and the websites you visit
- Access your data on all websites
- Detect your physical location

Figure 3 Polymorphic warning design variants.
(a) Original warning screenshot; **(b)** Color of text variation; **(c)** Highlight of text variation; **(d)** Signal word variation; **(e)** Pictorial signals variation; **(f)** Ordering of options variation; **(g)** Color variation; **(h)** Size variation (3x Larger); **(i)** Contrast variation; **(j)** Border variation.

Table 5 Latent growth curve parameter results

	Intercept (I)	*Slope (S)*	*I~polymorphic*	*S~polymorphic*
Estimate	11.073	–0.523	0.142	0.139
Standard error	0.531	0.061	0.339	0.039
z-Value	20.865	–8.592	0.419	3.526
P-value	*P*<0.001	*P*<0.001	*P*> 0.05	*P*<0.01

fixations is roughly equivalent to the number of 16.66 ms time periods that the person was gazing at the area of interest. Figure 5 plots the Lowess curve (a plotting method for fitting a smooth curve between two variables) for the number of fixations over time on the warning. Before the analysis, a square-root transformation was performed on the number of fixations (a typical transformation for counts) to increase linearity of the trend lines.

The latent growth curve model was specified for the number of fixations on the warning over time. In the model, the square root of the number of fixations on the warning was included as the observed values at each time step (D1 to D10 successively in Figure 6). Relationships from the intercept (*I*) and slope (*S*) latent variables were specified to each time step. A dummy variable was included to indicate whether the warning was polymorphic or static (polymorphic = 1, static = 0), and to allow us to explore whether the intercept or slope was statistically different between the treatment groups.

Figure 4 Tobii T120 eye tracker with integrated monitor.

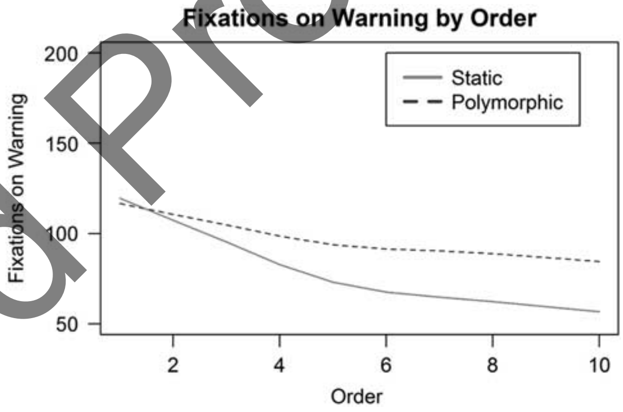


Figure 5 Growth trend of fixations on warning.

The analysis is shown in Table 5. The slope of warning fixation over time was significantly negative, indicating that people gazed less at warnings over successive viewings (–0.496, *P*<0.001, H1 supported). However, the effect of polymorphic warnings on the slope was significantly positive, indicating that the slope for polymorphic warnings was less negative and decreased more gradually (0.092, *P*<0.01, H2 supported).

Discussion

This study makes several important contributions – conceptual, empirical, and practical – to the study of security messages and to behavioral information security generally, as elaborated below.

Conceptual contributions

First, we have presented a research agenda comprising four questions for researching users' reception of security messages using NeuroIS methods. Each question was drawn

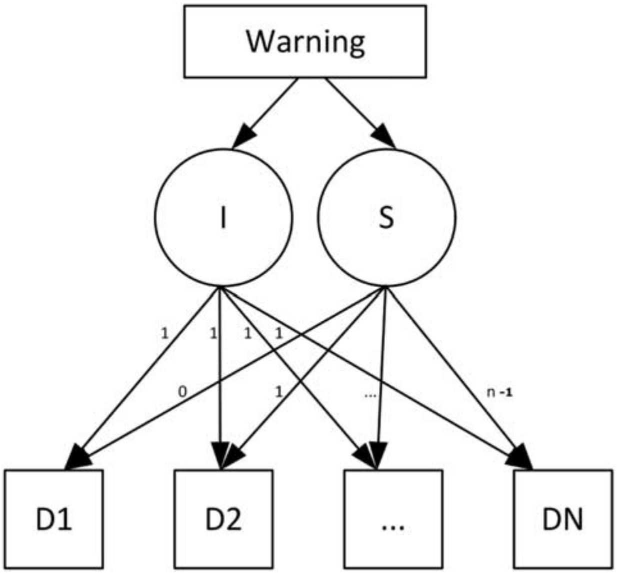


Figure 6 Latent growth curve model for both analyses (Fixations on Warning and Fixations on Warning Text).
Note: '*I*' is the model intercept, and '*S*' is the slope. 'Di' is the display count of the warning. The numbers on the path indicate the weight of the intercept and slope at a given time period. For example, the estimate of warning fixations at D2 would be $y = S(1)+I(1)$ and at D3 would be $y = S(2)+I(1)$.

from an extensive review of the IS, HCI, and NeuroIS literatures. This agenda is a valuable resource to the behavioral information security community because it (1) identifies several potentially fruitful streams of research, and (2) identifies a variety of NeuroIS methods that are well suited to investigating each question. Thus, this research agenda can assist scholars in initiating research on behavioral processing of security messages.

Second, this article advocates a multidisciplinary approach to the study of security messages, integrating behavioral information security and cognitive neuroscience to increase our understanding beyond that of traditional experimental observation and self-reporting. Our research questions are amenable to a NeuroIS lens because habituation, stress, fear, and dual-task interference are deeply rooted in our psyches and affect our behavior unconsciously, and these factors are difficult to capture without neurophysiological measures (Riedl *et al*, 2014). Using NeuroIS methods to directly observe the brain can afford insights about IS phenomena that could not be gained otherwise (Dimoka *et al*, 2011).

Empirical contributions

Although the purpose of our illustrative experiment was primarily to demonstrate how NeuroIS methods can be applied to investigate the research questions, the results also make empirical contributions. Although the literature has frequently cited habituation to warnings as a problem, few studies have empirically examined habituation. The studies that did used indirect measures, such as warning click-through rates (Bravo-Lillo *et al*, 2013). An exception is Anderson *et al* (2015), who used fMRI to show how habituation occurs in the brain, and demonstrated that their polymorphic design is effective in reducing habituation. This study provides additional empirical support for those findings.

Our illustrative experiment demonstrates how multiple NeuroIS tools can complement each other and compensate for weaknesses inherent in individual methods. In the case of Anderson *et al* (2015), fMRI excels in its ability to spatially locate neural activity in the brain. However, this method required concessions in ecological validity, as participants were required to view the warnings while lying down in an MRI scanner. In contrast, eye tracking was used to non-invasively obtain precise eye movements as a behavioral measure for habituation while participants viewed security warnings in a typical desktop computing configuration. Thus, eye tracking was used to triangulate the results of the fMRI experiment, and enhance the ecological results of Anderson *et al* (2015).

The experiment's results prove the value of our NeuroIS research agenda for security messages (Nunamaker & Briggs, 2012), demonstrating the kind and quality of insights that can be gained by pursuing our proposed research questions. Our initial foray into the question of how habituation to security messages can be reduced suggests related questions. For example, it is unknown how habituation to security messages changes over time, as existing studies have only examined the onset of habituation within a period of a few minutes (Brustoloni & Villamarín-Salomón, 2007; Bravo-Lillo *et al*, 2013). Our results illustrate the promise of NeuroIS to increase our understanding of users' reception to security messages, leading to the development of more complete behavioral theories and guiding the design of more effective security messages (Dimoka *et al*, 2012).

Implications for practice

Our findings have important implications for practice in the development of interventions to reduce habituation to security warnings. Rather than relying only on interventions such as SETA programs, which encourage greater vigilance (Karjalainen & Siponen, 2011), our results suggest that an effective complementary measure is to develop UI-design artifacts that reduce habituation in the brain, such as the polymorphic warning developed in this study. Rather than requiring explanations and training that can require hours or days, our polymorphic artifact elicits positive effects in milliseconds. In providing this benefit, the polymorphic warning artifact in this study is unobtrusive and imposes no additional cost to the user. In contrast, other techniques for curbing habituation, such as imposing a time delay on security warnings before they can be dismissed (Brustoloni & Villamarín-Salomón, 2007; Bravo-Lillo *et al*, 2013), impose a cost that can be considerable over time and when aggregated over a large workforce or population (Herley, 2009). Our polymorphic warning artifact is simple and cost-effective to implement in virtually any kind of system. With minimal additional graphical design and programming necessary to create a few variations, polymorphic warnings can help prevent habituation to warnings.

Conclusion

NeuroIS has the potential to provide new understanding of how users respond to security messages, a problem that has long vexed security researchers (Adams & Sasse, 1999; Bravo-Lillo *et al*, 2013). In this article, we presented a NeuroIS research agenda to examine four key neurological factors relating to how users receive and process security messages. Further, we presented the results of an experiment that illustrate the value and kinds of insights that can be derived using a NeuroIS approach. By pursuing these research questions, IS security scholars can significantly advance our understanding of security messages and how to design them to be more effective.

About the authors

Bonnie Brinton Anderson is an Associate Professor of Information Systems and Director of the Master of Information Systems Management (MISM) program in the Marriott School of Management at Brigham Young University. She received her Ph.D. from Carnegie Mellon University. She also has an MPhil from CMU as well as BS and MAcc degrees from BYU. She was a consultant for Accenture prior to returning to graduate school for her Ph.D. Her work has been published in *Journal of the Association for Information Systems, and Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI), Decision Support Systems, Electronic Commerce Research, Expert Systems with Applications; Electronic Commerce Research, Communications of the ACM, Information Sciences, IEEE Transactions: Systems, Men, and Cybernetics, The Journal of Systems and Software*, and other outlets. She currently researches the intersection of decision neuroscience and behavioral information security.

Anthony Vance is as an Associate Professor of Information Systems in the Marriott School of Management of Brigham Young University. He has earned Ph.D. degrees in Information Systems from Georgia State University, USA; the University of Paris –Dauphine, France; and the University of Oulu, Finland. His previous experience includes working as a visiting research professor in the Information Systems Security Research Center at the University of Oulu. His work is published in outlets such as *MIS Quarterly, Journal of Management Information Systems, Journal of the Association for Information Systems, European Journal of Information Systems, Journal of the American Society for Information Science and Technology, and Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI). His research focuses on behavioral and neuroscience applications to information security. He currently is an associate editor at MIS Quarterly and serves on the editorial board of Journal of the Association for Information Systems.

Brock Kirwan received his Ph.D. in Psychological and Brain Sciences from Johns Hopkins University in 2006. He has a decade of experience conducting fMRI scans with patient populations at Johns Hopkins University, the University of California, San Diego, the University of Utah, and now BYU. He has published numerous papers reporting fMRI and neuropsychological results in journals such as *Science, Proceedings of the National Academy of Sciences, Neuron, and the Journal of Neuroscience*.

David Eargle is a doctoral candidate in the Information Systems and Technology Management Area at the University of Pittsburgh in the Katz Graduate School of Business. He completed a joint baccalaureate-master's program in information systems management at Brigham Young University, completing the IS Ph.D. preparation program and graduating magna cum laude with University Honors. His research interests include human-computer interaction and information security. He has coauthored several articles in these areas using neurophysiological and other methodologies in outlets such as the *Journal of the Association for Information Systems, the International Conference on Information Systems, and the Hawaii International Conference on System Sciences, along with the Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI).

Jeffrey L. Jenkins is an Assistant Professor of Information Systems at the Marriott School of Management, Brigham Young University. He graduated with a Ph.D. in Management Information Systems from the University of Arizona. His active research includes human-computer interaction and behavioral information security. In a human-computer interaction context, his research explores how to infer human states using computer input devices such as the computer mouse, keyboard, or touchscreen. His research has been published in various journals and conference proceedings, including *MIS Quarterly, Journal of Management Information Systems, Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI), Computers in Human Behavior*, and others. Prior to earning his Ph.D., he was a software engineer in both the public and private sectors.

References

Abbasi A, Zhang Z, Zimbra D, Chen H and Nunamaker JJF (2010) Detecting fake websites: the contribution of statistical learning theory. *MIS Quarterly* **34**(**3**), 435–461.

Adams A and Sasse MA (1999) Users are not the enemy. *Communications of the ACM* **42**(**12**), 40–46.

Akhawe D and Felt AP (2013) Alice in warningland: a large-scale field study of browser security warning effectiveness. In *Proceedings of the 22nd USENIX conference on Security* (Sam K, Ed), pp 257–272, USENIX Association, Washington DC.

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

Anderson B, Kirwan B, Jenkins J, Eargle D, Howard S and Vance A (2015) How polymorphic warnings reduce habituation in the brain –insights from an fMRI study. In *ACM Conference on Human Factors in Computing Systems (CHI)* (Kim J and Begole B, Eds), ACM, Seoul, Korea.

Ayyagari R, Grover V and Purvis R (2011) Technostress: technological antecedents and implications. *MIS Quarterly* **35**(**4**), 831–858.

Bakker A, Kirwan CB, Miller M and Stark CEL (2008) Pattern separation in the human hippocampal CA3 and dentate gyrus. *Science* **319**(**5870**), 1640–1642.

Beck MR, Peterson MS and Angelone BL (2007) The roles of encoding, retrieval, and awareness. *Memory & Cognition* **35**(**4**), 610–620.

Benbasat I, Dimoka A, Pavlou PA and Qiu L (2010) Incorporating social presence in the design of the anthropomorphic interface of recommendation agents: insights from an fMRI study. In *ICIS 2010 Proceedings* (Lacity M, March S and Niederman F, Eds), AIS, St. Louis, MO.

Bench CJ, Frith CD, Grasby PM, Friston KJ, Paulesu E and Frackowiak RSJ *et al* (1993) Investigations of the functional anatomy of attention using the stroop test. *Neuropsychologia* **31**(**9**), 907–922.

Blanchard RJ and Blanchard DC (1994) Opponent environmental targets and sensorimotor systems in aggression and defence. In *Ethology and Psychopharmacology* (Cooper SJ and Hendrie CA, Eds), pp 133–157, Wiley, Chichester, UK.

Boss SR, Galletta DF, Lowry PB, Moody GD and Polak P (2015) What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly* **39**(**4**), 837–864.

Braun CC, Greeno B and Silver NC (1994) Differences in behavioral compliance as a function of warning color. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pp 379–383, SAGE Publications, Nashville, Tennessee.

Braun CC and Silver NC (1995) Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance. *Ergonomics* **38**(**11**), 2207–2220.

Bravo-Lillo C, Cranor LF, Downs J, Komanduri S and Sleeper M (2011) Improving computer security dialogs. In *Proceedings of the 13th IFIP TC 13 International Conference on Human-Computer Interaction – Volume 6949 Part IV* (CAMPOS P, GRAHAM N, JORGE J, NUNES N, PALANQUE P and WINCKLER M, Eds), pp 18–35, Springer-Verlag, Lisbon, Portugal.

Bravo-Lillo C *et al* (2013) Your attention please: designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Cranor L, Ed), pp 1–12, ACM, Newcastle, UK.

Brod C (1984) *Technostress: The Human Cost of the Computer Revolution*. Addison-Wesley, Reading, MA.

Brustoloni JC and Villamarín-Salomón R (2007) Improving security decisions with polymorphic and audited dialogs. In *Proceedings of the Third symposium on Usable Privacy and Security (SOUPS 2007)* (Cranor L, Ed), pp 76–85, ACM, New York, NY.

Cacioppo JT, Martzke JS, Petty RE and Tassinary LG (1988) Specific forms of facial EMG response index emotions during an interview: from Darwin to the continuous flow hypothesis of affect-laden information processing. *Journal of Personality and Social Psychology* **54**(**4**), 592–604.

Castellina E, Corno F and Pellegrino P (2008) Integrated speech and gaze control for realistic desktop environments. In *Proceedings of the 2008 Symposium on Eye Tracking Research & Applications* (Räihä K-J and Duchowski AT, Eds), pp 79–82, ACM, Savannah, GA.

Chen MC, Anderson JR and Sohn MH (2001) What can a mouse cursor tell us more?: correlation of eye/mouse movements on web browsing. In *CHI '01 Extended Abstracts on Human Factors in Computing Systems*, (Jacko J and Sears A, Eds), pp 281–282, ACM, Seattle, Washington DC.

Conti G, Ahamad M and Stasko J (2005) Attacking information visualization system usability overloading and deceiving the human. In *Proceedings of the 2005 Symposium on Usable Privacy and Security* (Cranor L and Zurko ME, Eds), pp 89–100, ACM, Menlo Park, CA.

Cooper CL, Dewe PJ and O'driscoll MP (2001) *Organizational Stress: A Review and Critique of Theory, Research, and Applications*. Sage, Thousand Oaks, CA.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M and Baskerville R (2013) Future directions for behavioral information security research. *Computers & Security* **32**(**1**), 90–101.

Cui X, Bray S, Bryant DM, Glover GH and Reiss AL (2011) A quantitative comparison of nirs and fMRI across multiple cognitive tasks. *NeuroImage* **54**(**4**), 2808–2821.

Dawson ME, Schell AM and Courtney CG (2011) The skin conductance response, anticipation, and decision-making. *Journal of Neuroscience, Psychology, and Economics* **4**(**2**), 111–116.

De Keukelaere F, Yoshihama S, Trent S, Zhang Y, Luo L and Zurko ME (2009) Adaptive security dialogs for improved security behavior of users. In *Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part I* (Gross T *et al*, Eds), pp 510–523, Springer-Verlag, Uppsala, Sweden.

Dhamija R and Tygar JD (2005) The battle against phishing: dynamic security skins. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, (Cranor L and Zurko ME, Eds), pp 77–88, ACM, Menlo Park, CA.

Dhamija R, Tygar JD and Hearst M (2006) Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Olson G, Rodden T and Grinter R, Eds), pp 581–590, ACM, Montréal, Canada.

Dickerson SS and Kemeny ME (2004) Acute stressors and cortisol responses: a theoretical integration and synthesis of laboratory research. *Psychological Bulletin* **130**(**3**), 355–391.

Dimoka A (2010) What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly* **34**(**2**), 373–396.

Dimoka A (2012) How to conduct a functional magnetic resonance (fMRI) study in social science research. *MIS Quarterly* **36**(**3**), 811–840.

Dimoka A *et al* (2012) On the use of neurophysiological tools in IS research: developing a research agenda for NeuroIS. *MIS Quarterly* **36**(**3**), 679–702.

Dimoka A, Pavlou PA and Davis FD (2011) Research commentary-NeuroIS: the potential of cognitive neuroscience for information systems research. *Information Systems Research* **22**(**4**), 687–702.

Downs JS, Holbrook MB and Cranor LF (2006) *Decision Strategies and Susceptibility to Phishing Proceedings of the Second Symposium on Usable Privacy and Security* (Cranor L, Karat C-M and Smetters D, Eds), ACM, Pittsburgh, Pennsylvania, pp 79–90.

Drake CE, Oliver JJ and Koontz EJ (2004) *Anatomy of a Phishing Email*, In *Conference on Email and Anti-Spam,* CEAS, Mountain View, CA.

Duncan J and Coltheart M (1987) *Attention and Reading: Wholes and Parts in Shape Recognition – A Tutorial Review*. England: Lawrence Erlbaum Associates, Hillsdale, NJ.

Dux PE, Ivanoff J, Asplund CL and Marois R (2006) Isolation of a central bottleneck of information processing with time-resolved fMRI. *Neuron* **52**(**6**), 1109–1120.

D'arcy J, Herath T and Shoss M (2014) Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems* **31**(**2**), 285–318.

Egelman S, Cranor LF and Hong J (2008) You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Czerwinski M and Lund A, Eds), pp 1065–1074, ACM, Florence, Italy.

Egelman S, Sotirakopoulos A, Muslukhov I, Beznosov K and Herley C (2013) *Does My Password Go Up to Eleven? The Impact of Password Meters on Password Selection*, In *ACM Conference on Human Factors in Computing Systems (CHI)* (Mackay WE, Ed), ACM, Paris, France, pp 2379–2388.

Ekman P, Rolls ET, Perrett DI and Ellis HD (1992) Facial expressions of emotion: an old controversy and new findings [and discussion]. *Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences* **335**(**1273**), 63–69.

Eysenck MW, Derakshan N, Santos R and Calvo MG (2007) Anxiety and cognitive performance: attentional control theory. *Emotion* **7**(**2**), 336–353.

Felt AP, Ha E, Egelman S, Haney A, Chin E and Wagner D (2012) Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Cranor L, Lipford H and Beznosov K, Eds), pp 3:1–3:14, ACM.

Felt AP, Reeder RW, Almuhimedi H and Consolvo S (2014) *Experimenting at Scale with Google Chrome's SSL Warning*, In *ACM Conference on Human Factors in Computing Systems (CHI)* (Jones M and Palanque P, Eds), ACM, Toronto, Canada, pp 2667–2670.

Fichman RG, Gopal R, Gupta A and Ransbotham S (2014) Call for papers: special issue on ubiquitous IT and digital vulnerabilities. *Information Systems Research.* [WWW document] http://pubsonline.informs.org/page/isre/calls-for-papers (accessed 13 November 2014).

Floyd DL, Prentice-Dunn S and Rogers RW (2000) A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* **30**(**2**), 407–429.

Foltz CB, Schwager PH and Anderson JE (2008) Why users (fail to) read computer usage policies. *Industrial Management & Data Systems* **108**(**6**), 701–712.

Freeman JB and Ambady N (2010) Mousetracker: software for studying real-time mental processing using a computer mouse-tracking method. *Behavior Research Methods* **42**(**1**), 226–241.

Frijda NH (1986) *The Emotions*. Cambridge University Press, Cambridge, New York.

Furnell S and Clarke N (2012) Power to the people? The evolving recognition of human aspects of security. *Computers & Security* **31**(**8**), 983–988.

Gartner (2013) Gartner says worldwide security market to grow 8.7 percent in 2013. [WWW document] http://www.gartner.com/newsroom/id/2512215 (accessed 29 January 2014).

Gefen D, Ayaz H and Onaral B (2014) Applying functional near infrared (fnir) spectroscopy to enhance mis research. *AIS Transactions on Human-Computer Interaction* **6**(**3**), 55–73.

Good N *et al* (2005) *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, In *Proceedings of the Symposium on Usable Privacy and Security* (Cranor L and Zurko ME, Eds), ACM, Pittsburgh, Pennsylvania,pp 43–52.

Grill-Spector K, Henson R and Martin A (2006) Repetition and the brain: neural models of stimulus-specific effects. *Trends in Cognitive Sciences* **10**(**1**), 14–23.

Grimes M, Jenkins JL and Valacich J (2013) Exploring the effect of arousal and valence on mouse interaction. In *International Conference on Information Systems* (Baskerville R and Chau M, Eds), AIS, Milan, Italy.

Guo Q and Agichtein E (2010) Towards predicting web searcher gaze position from mouse movements. In *CHI'10 Extended Abstracts on Human Factors in Computing Systems* (Mynatt E and Rodden T, Eds), pp 3601–3606, ACM, Austin, TX.

Haier RJ *et al* (1988) Cortical glucose metabolic rate correlates of abstract reasoning and attention studied with positron emission tomography. *Intelligence* **12**(**2**), 199–217.

Hannula DE, Althoff RR, Warren DE, Riggs L, Cohen NJ and Ryan JD (2010) Worth a glance: using eye movements to investigate the cognitive neuroscience of memory. *Frontiers in Human Neuroscience* (**4**), 1–16.

Hannula DE and Ranganath C (2009) The eyes have it: hippocampal activity predicts expression of memory in eye movements. *Neuron* **63** (**5**), 592–599.

Hehman E, Stolier RM and Freeman JB (2014) Advanced mouse-tracking analytic techniques for enhancing psychological science. *Psychological Science* **20**(**10**), 1183–1188.

Herath P, Klingberg T, Young J, Amunts K and Roland P (2001) Neural correlates of dual task interference can be dissociated from those of divided attention: an fMRI study. *Cerebral Cortex* **11**(**9**), 796–805.

Herley C (2009) So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms* (Somayaji A and Ford R, Eds), pp 133–144, ACM, Oxford, UK.

Herley C (2012) Why do Nigerian scammers say they are from Nigeria? In *Workshop on the Economics of Information Security (WEIS)* (Böhme R, Ed), WEIS, Berlin, Germany.

Hibbeln M, Jenkins J, Schneider C, Valacich J and Weinmann M (2014) Investigating the effect of insurance Fraud on mouse usage in human-computer interactions. In *Proceedings of the 2014 International Conference on Information Systems (ICIS 2014)*, (Karahanna E, Srinivasan A and Tan B, Eds), AIS, Auckland, New Zealand.

Hiraga CY, Garry MI, Carson RG and Summers JJ (2009) Dual-task interference: attentional and neurophysiological influences. *Behavioural Brain Research* **205**(**1**), 10–18.

Hong J (2012) The state of phishing attacks. *Communications of the ACM* **55**(**1**), 74–81.

Hsu M, Bhatt M, Adolphs R, Tranel D and Camerer CF (2005) Neural systems responding to degrees of uncertainty in human decision-making. *Science* **310**(**5754**), 1680–1683.

Hu Q, West R, Smarandescu L and Yaple Z (2014) Why individuals commit information security violations: neural correlates of decision processes and self-control. In *Hawaii International Conference on Systems Sciences* (Sprague R, Ed), IEEE, Waikoloa, HI.

Jenkins JL and Durcikova A (2013) What, I shouldn't have done that? The influence of training and just-in-time reminders on secure behavior. In *International Conference for Information Systems (ICIS)* (Baskerville R and Chau M, Eds), AIS, Milan, Italy.

Jenkins JL, Grimes M, Proudfoot J and Lowry PB (2013) Improving password cybersecurity through inexpensive and minimally invasive means: detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time warnings. *Information Technology for Development* **20**(**2**), 196–213.

Jiang Y (2004) Resolving dual-task interference: an fMRI study. *NeuroImage* **22**(**2**), 748–754.

Johnston A, Warkentin M and Siponen M (2015) An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* **39**(**1**), 113–134.

Johnston AC and Warkentin M (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* **34**(**3**), 549–566.

Kalsher M and Williams K (2006) Behavioral compliance: theory, methodology, and result. In *Handbook of Warnings* (Wogalter MS, Ed), pp 313–331, Lawrence Erlbaum Associates, Mahwah, NJ.

Kalsher MJ, Brewster BM, Wogalter MS and Spunar ME (1995) Hazard level perceptions of current and proposed warning sign and label panels. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 39(5), pp 351–355.

Kalsher MJ, Wogalter MS and Racicot BM (1996) Pharmaceutical container labels: enhancing preference perceptions with alternative designs and pictorials. *International Journal of Industrial Ergonomics* **18**(**1**), 83–90.

Kandel ER (2001) The molecular biology of memory storage: a dialogue between genes and synapses. *Science* **294**(**5544**), 1030–1038.

Karjalainen M and Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* **12**(**8**), 518–555.

Kemper D, Davis L, Fidopiastis C and Nicholson D (2007) Foundations for creating a distributed adaptive user interface. In *Foundations of Augmented Cognition* (Schmorrow D and Reeves L, Eds), Vol. 4565, pp 251–257, Springer, Berlin Heidelberg, Germany.

Kessem L (2012) Phishing in season: a look at online fraud in 2012. [WWW document] http://blogs.rsa.com/phishing-in-season-a-look-at-online-fraud-in-2012/ (accessed 13 November 2014).

Kleiss JA and Lane DM (1986) Locus and persistence of capacity limitations in visual information processing. *Journal of Experimental Psychology: Human Perception and Performance* **12**(**2**), 200–210.

Koch I (2009) The role of crosstalk in dual-task performance: evidence from manipulating response-code overlap. *Psychological Research* **73**(**3**), 417–424.

Krain AL, Wilson AM, Arbuckle R, Castellanos FX and Milham MP (2006) Distinct neural mechanisms of risk and ambiguity: a meta-analysis of decision-making. *NeuroImage* **32**(**1**), 477–484.

Kumaraguru P *et al* (2009) *School of Phish: A Real-World Evaluation of Anti-Phishing Training. Proceedings of Symposium on Usable Privacy and Security*, (Cranor L, Garfinkel S and Patrick A, Eds), ACM, Mountain View, CA.

Kumaraguru P, Rhee Y, Acquisti A, Cranor LF, Hong J and Nunge E (2007) *Protecting People From Phishing: The Design and Evaluation of an Embedded Training. Email System*, In *ACM Conference on Human Factors in Computing Systems (CHI)* (Rosson MB, Ed), ACM, San Jose, CA, pp 905–914.

Laughery KR, Young SL, Vaubel KP and JW Jr. BRELSFORD (1993) The noticeability of warnings on alcoholic beverage containers. *Journal of Public Policy & Marketing* **12**(**1**), 38–56.

Lerner JS and Keltner D (2001) Fear, anger, and risk. *Journal of Personality and Social Psychology* **81**(**1**), 146–159.

Lesch M (2006) Consumer product warnings: research and recommendations. In *Handbook of Warnings: Human Factors and Ergonomics* (Wogalter MS, Ed), pp 137–146, Lawrence Erlbaum Associates, Mahwah, NJ.

Lin E, Greenberg S, Trotter E, Ma D and Aycock J (2011) *Does Domain Highlighting Help People Identify Phishing Sites?* In *ACM Conference on Human Factors in Computing Systems (CHI)* (Mynatt E and Rodden T, Eds), ACM, Vancouver, British Columbia, Canada, pp 2075–2084.

Logan GD (1978) Attention in character-classification tasks: evidence for the automaticity of component stages. *Journal of Experimental Psychology* **107**(**1**), 32–63.

Loos P *et al* (2010) NeuroIS: neuroscientific approaches in the investigation and development of information systems. *Business & Information Systems Engineering* **2**(**6**), 395–401.

Lopatovska I and Arapakis I (2011) Theories, methods and current research on emotions in library and information science, information retrieval and human – computer interaction. *Information Processing & Management* **47**(**4**), 575–592.

Lowry PB *et al* (2013) Evaluating journal quality and the association for information systems senior scholars' journal basket via bibliometric measures: do expert journal assessments add value? *MIS Quarterly* **37**(**4**), 993–1012.

Luo XR, Zhang W, Burd S and Seazzu A (2013) Investigating phishing victimization with the heuristic – Systematic model: a theoretical framework and an exploration. *Computers & Security* **38**, 28–38.

Mach QH, Hunter MD and Grewal RS (2010) Neurophysiological correlates in interface design: an HCI perspective. *Computers in Human Behavior* **26**(**3**), 371–376.

Mahmood MA, Siponen M, Straub D and Rao HR (2008) Special issue call for papers: information systems security in a digital economy. *MIS Quarterly* **32**(**1**), 203–204.

Mahmood MA, Siponen M, Straub D, Rao HR and Raghu TS (2010) Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly* **34**(**3**), 431–433.

Mandiant (2013) *Apt1: Exposing One of China's Cyber Espionage Units.* Mandiant, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, accessed 4 December, 2015.

Maurer M-E, de Luca A and Kempe S (2011) *Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness*, In *Proceedings of the Symposium on Usable Privacy and Security* (Cranor L, Lipford H and Schechter S, Eds), ACM, Pittsburgh, Pennsylvania.

McArdle JJ and Nesselroade JR (2003) Growth curve analysis in contemporary psychological research. In *Handbook of Psychology* (Weiner IB, Schinka JA and Velicer WF, Eds), John Wiley & Sons, Hoboken, New Jersey.

McKendrick R, Ayaz H, Olmstead R and Parasuraman R (2014) Enhancing dual-task performance with verbal and spatial working memory training: continuous monitoring of cerebral hemodynamics with nirs. *NeuroImage* **85**(**3**), 1014–1026.

Meyer J (2006) Responses to dynamic warnings. In *Handbook of Warnings. Human Factors and Ergonomics* (Wogalter MS, Ed), pp 221–229, Lawrence Erlbaum Associates, Mahwah, NJ.

Minas R, Potter R, Dennis A, Bartelt V and Bae S (2014) Putting on the thinking cap: using NeuroIS to understand information processing biases in virtual teams. *Journal of Management Information Systems* **30**(4), 49–82.

Minnery BS and Fine MS (2009) Neuroscience and the future of human-computer interaction. *Interactions* **16**(**2**), 70–75.

Mitnick KD and Simon WL (2001) *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, Indianapolis, IN.

Moody G, Galletta D, Walker J and Dunn B (2011) Which phish get caught? An exploratory study of individual susceptibility to phishing. In *Proceedings of the 2011 International Conference on Information Systems (ICIS 2014)* (Galletta D and Liang T-P, Eds), AIS, Shanghai, China.

Moody GD and Galletta DF (2015) Lost in cyberspace: the impact of information scent and time constraints on stress, performance, and attitudes. *Journal of Management Information Systems* **32**(**1**), 192–224.

Moses SN *et al* (2007) Dynamic neural activity recorded from human amygdala during fear conditioning using magnetoencephalography. *Brain Research Bulletin* **71**(**5**), 452–460.

Motiee S, Hawkey K and Beznosov K (2010) *Do windows Users Follow the Principle of Least Privilege? Investigating User Account Control Practices* In *Proceedings of the Symposium on Usable Privacy and Security* (Cranor L, Patrick A and Schechter S, Eds), ACM, Redmond, Washington DC.

Neupane A, Saxena N, Kuruvilla K, Georgescu M and Kana R (2014) Neural Signatures of User-centered Security: An fMRI Study of Phishing, and Malware Warnings. *Procedings of the Network and Distributed System Security (NDSS) Symposium* (Bauer L, Ed), pp. 1–16.

Neupane A, Rahman ML, Saxena N and Hirshfield L (2015) A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)* (Kruegel C and Li N, Eds), Denver, CO, pp. 479–491.

Nunamaker Jr. JF and Briggs RO (2012) Toward a broader vision for information systems. *ACM Transactionson Management Information Systems* **2**(**4**), 1–12.

Ortiz de Guinea A and Markus ML (2009) Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *MIS Quarterly* **33**(**3**), 433–444.

Ortiz de Guinea A, Titah R and Léger P-M (2013) Measure for measure: a two study multi-trait multi-method investigation of construct validity in IS research. *Computers in Human Behavior* **29**(**3**), 833–844.

Pantev C *et al* (2004) Lateral inhibition and habituation of the human auditory cortex. *European Journal of Neuroscience* **19**(**8**), 2337–2344.

Pashler H (1994) Dual-task interference in simple tasks: data and theory. *Psychological Bulletin* **116**(**2**), 220–244.

Platt ML and Huettel SA (2008) Risky business: the neuroeconomics of decision making under uncertainty. *Nature Neuroscience* **11**(**4**), 398–403.

Plessow F, Schade S, Kirschbaum C and Fischer R (2012) Better not to deal with two tasks at the same time when stressed? Acute psychosocial stress reduces task shielding in dual-task performance. *Cognitive, Affective, & Behavioral Neuroscience* **12**(**3**), 557–570.

Polich J (2007) Updating p300: an integrative theory of p3a and p3b. *Clinical Neurophysiology* **118**(**10**), 2128–2148.

Proctor RW and Vu K-PL (2006) The cognitive revolution at age 50: has the promise of the human information-processing approach been fulfilled? *International Journal of Human-Computer Interaction* **21**(**3**), 253–284.

Raja F, Hawkey K, Hsu S, Wang K-LC and Beznosov K (2011) *A Brick Wall, A Locked Door, And A Bandit: A Physical Security Metaphor for Firewall warnings*, In *Proceedings of the Symposium on Usable Privacy and Security* (Cranor L, Lipford H and Schechter S, Eds), ACM, Pittsburgh, Pennsylvania.

Ramaswami M (2014) Network plasticity in adaptive filtering and behavioral habituation. *Neuron* **82**(**6**), 1216–1229.

Randolph A, Mccampbell L, Moore M and Mason S (2005) Controllability of galvanic skin response. In *11th International Conference on Human – Computer Interaction (HCII)*, Las Vegas, NV.

Rankin CH *et al* (2009) Habituation revisited: an updated and revised description of the behavioral characteristics of habituation. *Neurobiology of Learning and Memory* **92**(**2**), 135–138.

Raskin DC (1973) Attention and arousal. In *Electrodermal Activity in Psychological Research* (Prokasy W, Ed), pp 125–155, Academic Press, New York.

Rayner K (1998) Eye movements in reading and information processing: 20 years of research. *Psychological Bulletin* **124**(**3**), 372–422.

Rémy F, Wenderoth N, Lipkens K and Swinnen SP (2010) Dual-task interference during initial learning of a new motor task results from competition for the same brain areas. *Neuropsychologia* **48**(9), 2517–2527.

Riedl R (2012) On the biology of technostress: literature review and research agenda. *ACM SIGMIS Database* **44**(**1**), 18–55.

Riedl R *et al* (2010) On the foundations of NeuroIS: reflections on the gmunden retreat 2009. *Communications of the Association for Information Systems* **27**(**1**), 243–264.

Riedl R, Davis FD and Hevner AR (2014) Towards a NeuroIS research methodology: intensifying the discussion on methods, tools, and measurement. *Journal of the Association for Information Systems* **15**(**10**), i–xxxv.

Riedl R, Kindermann H, Auinger A and Javor A (2012) Technostress from a neurobiological perspective: system breakdown increases the stress hormone cortisol in computer users. *Business & Information Systems Engineering* **4**(**2**), 61–69.

Rogers RW and Prentice-Dunn S (1997) Protection motivation theory. In *Handbook of health Behavior Research 1: Personal and Social Determinants* (David S Gochman, Ed), pp 113–132, Springer, New York.

Rudin-Brown CM, Greenley MP, Barone A, Armstrong J, Salway AF and Norris BJ (2004) The design of child restraint system (CRS) labels and warnings affects overall CRS usability. *Traffic Injury Prevention* **5**(**1**), 8–17.

Sanders MS and McCormick EJ (1987) *Human Factors in Engineering and Design*, 7th edn, McGraw-Hill, New York.

Sankarpandian K, Little T and Edwards WK (2008) *Talc: Using Desktop Graffiti to Fight Software Vulnerability,* In *ACM Conference on Human Factors in Computing Systems (CHI)* (Czerwinski M and Lund A, Eds), ACM, Florence, Italy, pp 1055–1064.

Sarinopoulos I *et al* (2010) Uncertainty during anticipation modulates neural responses to aversion in human insula and amygdala. *Cerebral Cortex* **20**(**4**), 929–940.

Schechter SE, Dhamija R, Ozment A and Fischer I (2007) The emperor's new security indicators. In *IEEE Symposium on Security and Privacy, 2007* (Shands D, Pfitzmann B and McDaniel P, Eds), SP'07. pp 51–65, IEEE, Berkeley, CA.

Schellhammer S, Haines R and Klein S (2013) Investigating technostress *in situ*: understanding the day and the life of a knowledge worker using heart rate variability. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (Sprague R, Ed), pp 430–439, IEEE, Maui, Hawaii.

Schutter DJLG and van Honk J (2009) The cerebellum in emotion regulation: a repetitive transcranial magnetic stimulation study. *The Cerebellum* **8**(**1**), 28–34.

Searle BJ, Bright JEH and Bochner S (1999) Testing the 3-factor model of occupational stress: the impact of demands, control and social support on a mail sorting task. *Work & Stress* **13**(**3**), 268–279.

Sharek D, Swofford C and Wogalter M (2008) Failure to recognize fake internet popup warning messages. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Marras WS, Eds), pp 557–560, Sage Publications, New York.

Sheeran P (2002) Intention–Behavior relations: a conceptual and empirical review. *European Review of Social Psychology* **12**(**1**), 1–36.

Sheng S *et al* (2007) *Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish*, In *Proceedings of the Symposium on Usable Privacy and Security* (Cranor L, Hong J and Smetters D, Eds), ACM, Pittsburgh, Pennsylvania, pp 88–99.

Shimojo S, Simion C, Shimojo E and Scheier C (2003) Gaze bias both reflects and influences preference. *Nature Neuroscience* **6**(**12**), 1317–1322.

Sigman M and Dehaene S (2006) Dynamics of the central bottleneck: dual-task and task uncertainty. *PLoS Biology* **4**(**7**), e220.

Silver NC and Wogalter MS (1989) Broadening the range of signal words. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pp 555–559, SAGE Publications, Denver, CO.

Siponen M and Smith J (2014) Call for papers: IS security and privacy. *ICIS 2014: Building a better world through information systems.* [WWW document] http://icis2014.aisnet.org/index.php/submissions/tracks/14-is-security-and-privacy, accessed 30 June 2014.

Smith CN, Hopkins RO and Squire LR (2006) Experience-dependent eye movements, awareness, and hippocampus-dependent memory. *The Journal of Neuroscience* **26**(**44**), 11304–11312.

Sojourner RJ and Wogalter MS (1997) The influence of pictorials on evaluations of prescription medication instructions. *Drug Information Journal* **31**(**3**), 963–972.

Sonnentag S and Frese M (2003) Stress in organizations. In *Handbook of Psychology: Industrial and Organizational Psychology*, Vol. 12 Borman WC, Ilgen DR and Klimoski RJ, Eds), pp 453–491, John Wiley & Sons, Hoboken, NJ.

Sotirakopoulos A, Hawkey K and Beznosov K (2011) On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS)* (Cranor L, Lipford H and Schechter S, Eds), pp 3:1–3:18, ACM, Menlo Park, CA.

Straub D, Boudreau M-C and Gefen D (2004) Validation guidelines for IS positivist research. *Communications of the Association for Information Systems* **13**(**24**), 380–427.

Strawbridge JA (1986) The influence of position, highlighting, and imbedding on warning effectiveness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pp 716–720, SAGE Publications, Dayton, OH.

Sunshine J, Egelman S, Almuhimedi H, Atri N and Cranor LF (2009) Crying wolf: an empirical study of SSL warning effectiveness. In *SSYM'09 Proceedings of the 18th Conference on USENIX Security Symposium* (Monrose F, Ed), pp 399–416, Montreal, Canada.

Szameitat AJ, Schubert T, Müller K and von Cramon DY (2002) Localization of executive functions in dual-task performance with fMRI. *Journal of Cognitive Neuroscience* **14**(**8**), 1184–1199.

Tams S, Hill K, Ortiz de Guinea A, Thatcher J and Grover V (2014) NeuroIS – Alternative or complement to existing methods? Illustrating the holistic effects of neuroscience and self-reported data in the context of technostress research. *Journal of the Association for Information Systems* **15**(**10**), 1.

Tarafdar M, Gupta A and Turel O (2013) Special issue call for papers: dark side of IT use. *Information Systems Journal.* [WWW document] http://www.ncl.ac.uk/kite/news/item/information-systems-journal-special-issue-on-the-dark-side-of-it-use (accessed 13 November 2014).

Tombu M and Jolicœur P (2003) A central capacity sharing model of dual-task performance. *Journal of Experimental Psychology: Human Perception and Performance* **29**(**1**), 3–18.

Twyman NW, Lowry PB, Burgoon JK and Nunamaker JF (2015) Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *Journal of Management Information Systems* **31**(**3**), 106–137.

Ur B *et al* (2012) *How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation*, In USENIX Security Symposium (Kohno T, Ed), USENIX, Bellevue, Washington DC, pp 65–80.

van Turennout M, Ellmore T and Martin A (2000) Long-lasting cortical plasticity in the object naming system. *Nature Neuroscience* **3**(**12**), 1329–1334.

Vance A, Anderson BB, Kirwan CB and Eargle D (2014) Using measures of risk perception to predict information security behavior: insights from electroencephalography (EEG). *Journal of the Association for Information Systems* **15**(**10**), 679–722.

Vance A, Siponen M and Pahnila S (2012) Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management* **49**(**3–4**), 190–198.

Vaniea KE, Rader E and Wash R (2014) *Betrayed By Updates: How Negative Experiences Affect Future Security*, In *ACM Conference on Human Factors in Computing Systems (CHI)* (Jones M and Palanque P, Eds), ACM, Toronto, Canada, pp 2671–2674.

Verplanken B and Aarts H (1999) Habit, attitude, and planned behaviour: is habit an empty construct or an interesting case of goal-directed automaticity? *European Review of Social Psychology* **10**(**1**), 101–134.

Vigilante Jr. WJ and Wogalter M (2003) Effects of label format on knowledge acquisition and perceived readability by younger and older adults. *Ergonomics* **46**(**4**), 327–344.

Villamarín-Salomón RM and Brustoloni JC (2010) *Using Reinforcement to Strengthen Users' Secure Behaviors*, In *ACM Conference on Human Factors in Computing Systems (CHI)*, ACM, Atlanta, Georgia, pp 363–372.

vom Brocke J and Liang T-P (2014) Guidelines for neuroscience studies in information systems research. *Journal of Management Information Systems* **30**(**4**), 211–234.

Vredenburgh A and Zackowitz I (2006) Expectations. In *Handbook of Warnings* (Wogalter MS, Ed), pp 345–353, Lawrence Erlbaum Associates, Mahwah, NJ.

Warkentin M, Johnston AC and Vance A (2014) Call for papers: internet and the digital economy: innovative behavioral IS security and privacy research. *Hawaii International Conference on System Sciences* [WWW document] http://www.hicss.hawaii.edu/hicss_47/track/in/IN-Security.pdf, accessed 30 June 2014.

Warkentin M, Walden EA and Johnston AC (2012) Identifying the neural correlates of protection motivation for secure IT behaviors. In *Gmunden Retreat on NeuroIS 2012* (Davis F, Riedl R, vom Brocke J, Léger P-M and Randolph A, Eds), Gmunden, Austria.

Warkentin M and Willison R (2008) Special issue call for papers: behavioural and policy issues in information systems security. *European Journal of Information Systems* [WWW document] http://www.palgrave-journals.com/ejis/Promo-EJIS_InfoSec.pdf, accessed 30 June 2014.

Warkentin M and Willison R (2009) Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems* **18**(**2**), 101–105.

Warkentin M, Walden EA, Johnston AC and Straub DW (forthcoming) Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems.*

WASTELL D and NEWMAN M (1993) The behavioral dynamics of information system development: a stress perspective. *Accounting, Management and Information Technologies* **3**(**2**), 121–148.

WEBER R (2004) The grim reaper: the curse of e-mail. *MIS Quarterly* **28**(**3**), 3–14.

WELSH TN and ELLIOTT D (2004) Movement trajectories in the presence of a distracting stimulus: evidence for a response activation model of selective reaching. *The Quarterly Journal of Experimental Psychology Section A* **57**(**6**), 1031–1057.

WEST R (2008) The psychology of security. *Communications of the ACM* **51**(**4**), 34–40.

WHALEN PJ (1998) Fear, vigilance, and ambiguity: initial neuroimaging studies of the human amygdala. *Current Directions in Psychological Science* **7**(**6**), 177–188.

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

WOGALTER M and VIGILANTE Jr. WJ (2006) Attention switch and maintenance. In *Handbook of Warnings* (Wogalter MS, Ed), pp 245–266, Lawrence Erlbaum Associates, Mahwah, NJ.

WRIGHT RT and MARETT K (2010) The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. *Journal of Management Information Systems* **27**(**1**), 273–303.

WU M, MILLER RC and GARFINKEL SL (2006) Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Olson G, Rodden T and Grinter R, Eds), pp 601–610, ACM, Montreal, Canada.

YEE K-P (2004) Aligning security and usability. *Security & Privacy, IEEE* **2**(**5**), 48–55.

YOUNG SL (1991) Increasing the noticeability of warnings: effects of pictorial, color, signal icon and border. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pp 580–584, SAGE Publications, San Francisco, VA.

YOUNG SL and WOGALTER M (1990) Effects of conspicuous print and pictorial icons on comprehension and memory of instruction manual warnings. *Human Factors* **32**(**6**), 637–649.

Appendix A

Security messages taxonomy

Figure A1 depicts a taxonomy of security messages along with specific examples, which consistent with our definition, may be offensive or defensive in nature. Our scheme classifies security messages according to three primary dimensions: (1) immediacy, (2) relevancy, and (3) complexity. Immediacy refers to the extent to which a message can be deferred. At one extreme, modal software dialogs by design interrupt the user's workflow until the message has been processed (Egelman *et al*, 2008). On the other end of the spectrum, security advisories are often in e-mail form, which can be easily set aside for later processing (Weber, 2004). Immediacy has important implications for how security messages are processed because users are less likely to act on messages that can be deferred (Egelman *et al*, 2008). This is why Web browsers have recently emphasized modal warnings that interrupt the user rather than passive indicators that reside in the chrome of the browser and are easily overlooked (Akhawe & Felt, 2013).

Relevancy concerns the applicability of a security message to the workflow or task that the user is engaged in.

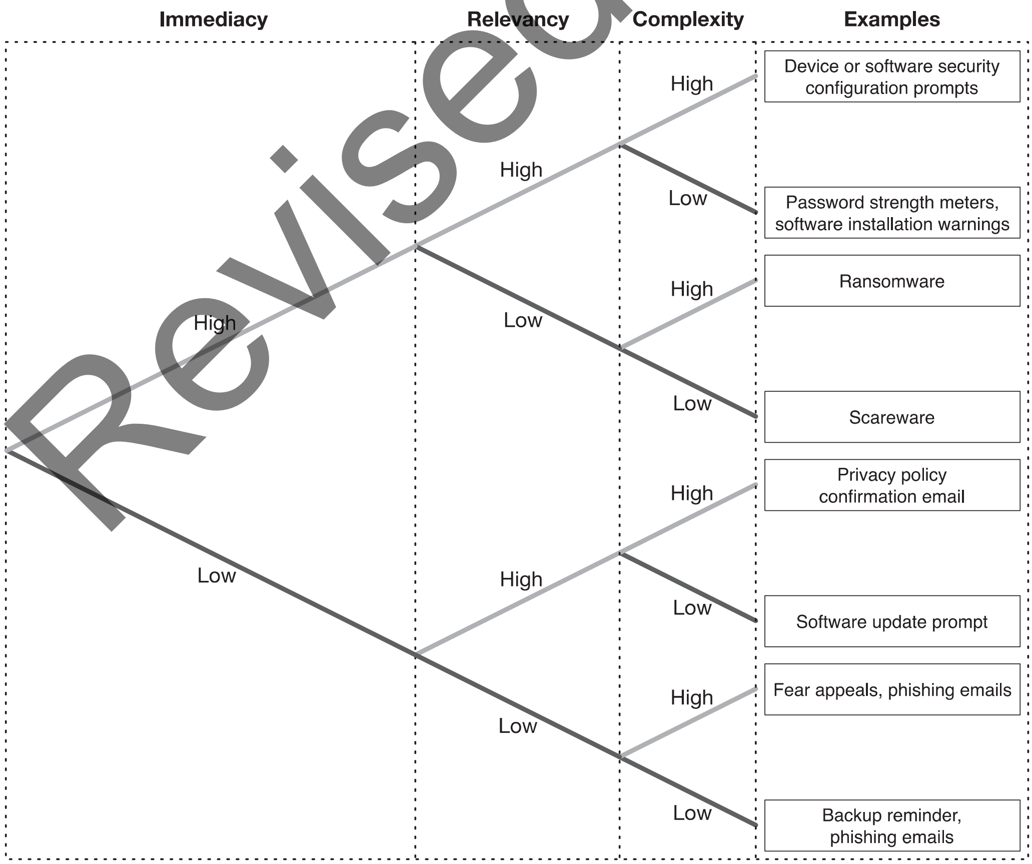


Figure A1 Taxonomy of security messages.

Users are more likely to process security messages that are anticipated or clearly applicable to the present task (Vredenburgh & Zackowitz, 2006). In contrast, security messages that have little connection to a user's current activity are less easily processed because they require users to switch attention from the task at hand (Meyer, 2006). This is one reason why information security policies are less likely to be followed if they are separate from a user's routine work activities (Vance *et al*, 2012). This is also why spear-phishing attacks that are targeted to a user's work are much more effective (Luo *et al*, 2013).

Complexity describes the informational density of a security message, the mental effort required to process the message, or both. Security messages can be very sparse, such as software dialogs that contain only a few words. Conversely, other security messages contain multiple sub-arguments, such as fear appeals, which convey (1) the severity of a threat, (2) the user's susceptibility to a threat, (3) the efficacy of a suggested response, and (4) the user's self-efficacy to enact the protective action (Johnston & Warkentin, 2010; Johnston *et al*, 2015). More complex still are legalistic, acceptable-use policies that users find intractable (Foltz *et al*, 2008).

For simplicity of presentation, the taxonomy depicts a binary, high/low classification for each dimension, but each message falls along a gradient for each dimension. Some types of security messages (e.g., phishing e-mails) are flexible enough to fall into several categories. For example, phishing e-mails may offer a single link as bait or be long and abstruse like a Nigerian 419 scam (Herley, 2012). The hierarchical ordering of the taxonomy suggests a precedence among the dimensions, with immediacy being the most important factor in whether a user processes a message because messages high in immediacy can interrupt the user and demand attention (Lesch, 2006; Egelman *et al*, 2008). We consider relevancy to be the next most important factor, given that if a message is determined to be highly relevant, a user will invest time and effort to process the message, regardless of complexity (Vredenburgh & Zackowitz, 2006).

Appendix B

Listing of articles identified in the literature review

Table B1 Selection of research areas relating to security messages from AIS-6, HCI sources

Citation	*Outlet*	*Type of security message*	*Supported research questions*
Anderson & Agarwal (2010)	*MIS Quarterly*	Effect of persuasive general public security notices on security intentions and attitudes	Attitudes and beliefs (concern about security threats, response-efficacy, self-efficacy), norms
Johnston & Warkentin (2010)	*MIS Quarterly*	Fear appeals encouraging antispyware installation	Intention–behavior, fear
Felt *et al* (2014)	*CHI*	SSL warnings	Fear, attention
Vaniea *et al* (2014)	*CHI*	Program update (patch) prompts	Fear, uncertainty, comprehension
Egelman *et al* (2013)	*CHI*	Password strength meter	Motivation (encouragement), comprehension
Lin *et al* (2011)	*CHI*	Phishing security, anti-phishing user interfaces	Deception detection
Villamarín-Salomón & Brustoloni (2010)	*CHI*	Handling of phishing e-mail messages	Habituation, motivation (rewards)
Sankarpandian *et al* (2008)	*CHI*	Application patch process manager	Comprehension, attention, motivation (persistent security notifications)
Egelman *et al* (2008)	*CHI*	Phishing warnings	Habituation, comprehension, attitudes and beliefs (trust in the warning, perceived threat likelihood, threat severity, risk-avoidance)
Kumaraguru *et al* (2007)	*CHI*	Phishing education system	Deception detection
Dhamija *et al* (2006)	*CHI*	Browser-based cues and security indicators in a phishing context	Attention, comprehension
Crossler *et al* (2013)	*Computers & Security*	Fear appeals, interactive security prompts, malware warnings	Fear, intention–behavior
Bravo-Lillo *et al* (2013)	*SOUPS*	Browser plugin installation warning	Habituation
Felt *et al* (2012)	*SOUPS*	Android app installation (malware)	Attention, comprehension, technostress, information processing (unawareness)
Raja *et al* (2011)	*SOUPS*	Firewall warnings	Comprehension
Maurer *et al* (2011)	*SOUPS*	Tool-tip alert dialogs	Habituation
Sotirakopoulos *et al* (2011)	*SOUPS*	SSL warnings	Intention–behavior, habituation

Table B1: (*Continued*)

Citation	*Outlet*	*Type of security message*	*Supported research questions*
Motiee *et al* (2010)	*SOUPS*	Windows UAC, malware	Attention, comprehension
Kumaraguru *et al* (2009)	*SOUPS*	anti-phishing training	Deception detection, demographics (gender, age)
Sheng *et al* (2007)	*SOUPS*	Anti-phishing training	Deception detection
Brustoloni & Villamarín-Salomón (2007)	*SOUPS*	Open e-mail attachment dialogs	Habituation, motivation (accountability)
Wu *et al* (2006)	*SOUPS*	Anti-phishing toolbar	Attention, deception detection
Downs *et al* (2006)	*SOUPS*	Phishing	Deception detection
Good *et al* (2005)	*SOUPS*	Installing software with spyware, installation warnings, End User License Agreement	Comprehension, fear, attention
Dhamija & Tygar (2005)	*SOUPS*	Phishing browser warnings	Deception detection, technostress, information processing (cognitive demands)
Conti *et al* (2005)	*SOUPS*	Attack vectors against visual intrusion detection systems	Deception detection, technostress, attitudes and beliefs (trust), information processing (cognitive demands)
Akhawe & Felt (2013)	*USENIX*	Browser malware, phishing, and SSL warnings	Habituation, attitudes and beliefs (annoyance), technostress, information processing (security messages as interruptions)
Ur *et al* (2012)	*USENIX*	Password strength meters	Attention, fear, motivation (encouragement), attitudes and beliefs (annoyance, laziness), technostress, information processing (cognitive demands)
Sunshine *et al* (2009)	*USENIX*	SSL warnings	Habituation, comprehension

Table B2 Expanded and reduced lists of extracted research questions from AIS-6 and HCI computer science literature

Expanded research question	*n*	*Reduced research question*	*n*
Comprehension	10	Comprehension	18
Attention	7	Attention/habituation	22
Deception detection	8		
Habituation	8		
Fear	6	Fear	6
Stress/technostress	5	Stress	5
Intention–behavior	3	Intention–behavior	3
Information processing (cognitive demands)	3	Dual-task interference	6
Information processing (security messages as interruptions)	2		
Information processing (unawareness)	1		
Attitudes and beliefs (annoyance)	2	Attitudes and beliefs, motivations	10
Attitudes and beliefs (laziness)	1		
Attitudes and beliefs (concern about security threats, response-efficacy, self-efficacy)	1		
Attitudes and beliefs (perceived threat likelihood, threat severity, risk avoidance)	1		
Attitudes and beliefs (trust)	2		
Motivation (encouragement)	2		
Motivation (accountability)	1		
Motivation (persistent security notifications)	1		
Motivation (rewards)	1		
Gender differences	1	Gender differences	1
Norms	1	Norms	1
Uncertainty	1	Uncertainty	1

Table B3 IS security issues and opinions, call for papers, and research agendas

Citation	*Outlet*	*Type of paper*	*Supported research questions of interest*	*Notes*
Crossler *et al* (2013)	*Computers & Security*	Research agenda	Fear, intention–behavior gap, security policy compliance	
Siponen & Smith (2014)	*European Journal of Information Systems*	Issues and opinions	Intention–behavior gap, insider threat	Highlights the importance of improving practical relevance for IS security field surveys, suggesting that such improvements can lessen data measurement issues associated with the intention–behavior gap.
Warkentin & Willison (2009)	*European Journal of Information Systems*	Issues and opinions	Intention–behavior gap, insider threat	Focus on the insider threat
Warkentin & Willison (2008)	*European Journal of Information Systems*	Special issue CFP	Intention–behavior gap, insider threat	Focus on the insider threat (volitional and accidental security policy violations)
Warkentin *et al* (2014)	*Hawaii International Conference on System Sciences*	Conference CFP	Intention–behavior gap, insider threat, security-policy compliance	
Siponen & Smith (2014)	*ICIS 2014*	Conference CFP	Insider threat, policy compliance	Emphasizes the practical importance of research. Behavioral security topics include insider threats (malicious and careless external attacks
Tarafdar *et al* (2013)	*Information Systems Journal*	Special issue CFP	Technostress, insider threat	
Fichman *et al* (2014)	*Information Systems Research*	Special issue CFP	Deceptive IT; irresponsible exposure of personal information through use of dangerous IT	Calls for research on the 'darker side' of IT for organizations, societies, and individuals. Two relevant topics of interest include 'dissemination of information with dangerous applications […] related to risky personal behavior' and 'information technology used for fraud and deception'
Mahmood *et al* (2010)	*MIS Quarterly*	Issues and opinions	Behavioral security, outsider threat	Heavy focus on calling for more research about information security attackers
Mahmood *et al* (2008)	*MIS Quarterly*	Special issue CFP	Behavioral security	Security from a management perspective as opposed to technical solutions (behavioral security)

Table B4 NeuroIS issues and opinions and research agendas

Citation	*Outlet*	*Literature stream-specific RQ*	*Triangulated RQ*	*Notes*
Riedl (2012)	*ACM SIGMIS Database*	Technostress	Technostress	
Loos *et al* (2010)	*Business & Information Systems Engineering*	Triangulate objective data with self-report, advance TAM (technostress, dis/engagement, cognitive absorption, etc.), gender differences, evaluate and inform design science (develop human–computer interfacing technology)	Intention–behavior gap, technostress, habituation, gender differences	Habituation RQ supported through focus on user engagement with systems
Riedl *et al* (2010)	*Communications of the Association for Information Systems*	Discussed in the context of studying TAM: cognition (absorption, workload, etc.), affective (enjoyment, anxiety), automatic processing. Discussed as general RQs: especially uncertainty, risk, and ambiguity. Trust and distrust. Gender	Technostress, fear, habituation, uncertainty, risk, trust, gender differences	Fear through affect emphasis; habituation through automatic processing emphasis
Dimoka *et al* (2011)	*Information Systems Research*	Intention–behavior (overcome self-report biases), deep emotions	Intention–behavior gap, fear, attention, uncertainty	
vom Brocke & Liang (2014)	*Journal of Management Information Systems*	Reduce self-reporting bias (intention–behavior gap), plus all security-relevant topics in special issue: technology acceptance, emotions, trust, stress	Intention–behavior gap, fear, technostress	
Dimoka *et al* (2012)	*MIS Quarterly*	Collect objective data (intention–behavior gap), deep or hidden emotions such as fear, IS adoption and use (including cognitive overload, anxiety, technostress), habitual systems interaction patterns. Decision making (uncertainty), online trust	Intention–behavior gap, fear, technostress, attention (engagement)	

Table B5 Support for RQs from NeuroIS issues and opinions and research agendas

Research question	*NeuroIS Supported?*	*Supporting papers (and notes)*	*Supporting arguments (summary)*
Attention/habituation	Yes	DLPFC, under the 'assessing Information and Cognitive Overload' section (Dimoka *et al*, 2012, p. 685) Attention in Section 1 'Localizing neural correlates of usability' (Dimoka *et al*, 2011) User engagement: (Loos *et al*, 2010) Heart rate (frequently EKG) to measure cognitive attention (Riedl *et al*, 2010, p. 246) Attention (vom Brocke & Liang, 2014, p. 222)	Attention and habituation can be an unconscious event. Measuring attention via self-report can interfere with the very thing that is being measured – it can break user engagement with the task at hand
Comprehension	Indirectly supported, via learning to comprehend	Use fMRI to study neural correlates of deception and eye tracking to study deception detection, and study 'how *learning* [about deception detection] can be achieved in fearful situations, such as phishing websites' (Dimoka *et al*, 2012, p. 687 (emphasis added)) Localize different types of learning (Dimoka *et al*, 2011, p. 9)	Comprehension may not be better measured using non-NeuroIS methods
Fear	Yes	Riedl *et al* (2010), Dimoka *et al* (2012), vom Brocke & Liang (2014)	Fear has deep, hidden emotional components that can be uncovered with NeuroIS
Stress	Yes, via technostress	Loos *et al* (2010), Riedl *et al* (2010), Dimoka *et al* (2012), Riedl (2012), vom Brocke & Liang (2014)	Stress (and by inclusion technostress) can be difficult to measure via self-report, because of deep components or participants' inability to answer
Dual-task interference	Yes	'Complex cognitive processes (e.g., cognitive overload)' (Dimoka *et al*, 2012, p. 680; vom Brocke & Liang, 2014, p. 221) Difficult-to-measure latent variables (Dimoka *et al*, 2011, p. 15)	Dual-task interference can be considered as a latent variable from a complex cognitive process
Attitudes and beliefs, motivations	Yes	'Antecedents of human behavior' (Dimoka *et al*, 2011; Dimoka *et al*, 2012; vom Brocke & Liang, 2014)	NeuroIS is appropriate if measurement of the attitude, belief, or motivation is otherwise subject to bias or occurs at an unconscious level
Intention–behavior	Yes	Yes, via the idea of collecting objective, unbiased data (Loos *et al*, 2010; Dimoka *et al*, 2011; Dimoka *et al*, 2012; vom Brocke & Liang, 2014)	NeuroIS is good for investigating this gap as it captures unbiased data
Gender differences	Yes	Loos *et al* (2010), Riedl *et al* (2010)	NeuroIS can uncover differences in brain activity between genders
Uncertainty	Yes	Uncertainty and ambiguity (Dimoka *et al*, 2011)	Uncertainty and ambiguity may have hidden neurophysiological correlates
Norms	Yes	'Antecedents of human behavior' (Dimoka *et al*, 2011; Dimoka *et al*, 2012; vom Brocke & Liang, 2014)	NeuroIS is appropriate as norms may influence an individual's choice unconsciously, or to the degree that self-reports would be biased