Spring 6-10-2017

MAKING CUES SALIENT: THE ROLE OF SECURITY AWARENESS IN SHAPING THREAT AND COPING APPRAISALS

Lennart Jaeger
German Graduate School of Management & Law, lennart.jaeger@ggs.de

Andreas Eckhardt
German Graduate School of Management & Law (GGS), andreas.eckhardt@ggs.de

MAKING CUES SALIENT: THE ROLE OF SECURITY AWARENESS IN SHAPING THREAT AND COPING APPRAISALS

Research in Progress

Jaeger, Lennart, German Graduate School of Management and Law, Heilbronn, Germany, lennart.jaeger@ggs.de

Eckhardt, Andreas, German Graduate School of Management and Law, Heilbronn, Germany, andreas.eckhardt@ggs.de

Abstract

The number of phishing e-mails sent to users' inboxes at organizations increases every year, putting users under constant threat of data or identity theft. In finding ways to motivate users to protect themselves and their organization from such threats, IS security researchers using protection motivation theory (PMT) have made notable contributions to the relationship between appraisal processes and adaptive responses. In this study, we argue that security awareness is the missing link that can explain what makes cues salient. To observe this link, we have recently conducted a multi-method experimental design including eye tracking, facial analysis, and survey components to shed light on the relationship between users' awareness and appraisal processes. Our study also contributes to prior literature by observing the effect of fear appeal manipulations on this relationship and the role of fear in user protection motivation. Additionally, we are able to uncover actual security-related behaviors.

Keywords: Information security, Phishing, Fear appeals, Security awareness.

1 Introduction

E-mails play an important role in today's information society by supporting and enabling information sharing and communication, but are also often misused to steal personal and financial information through phishing and spamming schemes and/or to spread viruses, worms, Trojan horses and malware (Herath et al., 2014). These security threats leave users vulnerable to identity theft or online fraud and can result in the alteration and corruption of data (Herath et al., 2014). In the face of such threats, users are confronted with a discrepant IT event (De Guinea, A. O. and Webster, 2013), which is a situation that entails a difference between what is expected and what is taking place (Louis and Sutton, 1991). Further examples for such an event could be a problem, a misunderstanding, or a difficulty with the applied IS (Tyre and Orlikowski, 1994). In the IS security context, such discrepant events can also be security messages, i.e., discrete communication designed to persuade users to either impair or improve their security status (Anderson et al., 2016). Malicious messages (e.g., phishing attacks) or protective messages (e.g., security warnings) represent both a threat and an opportunity for the user. They can be threatening because they affect the confidentiality and security of corporate data as well as users' privacy. But they also represent an opportunity for individual and organizational learning (Tyre and Orlikowski, 1994). The discrepant IT events are commonly modeled as the application of fear appeals in the form of persuasive messages warning users about potential threats and describing countermeasures (Floyd et al., 2000). Users appraise this event in a dynamic interaction between the individual and the discrepant event. As this situation develops, special focus lies on the adaptations the users perform in order to adapt to the new circumstances (Carver and Scheier, 1994). Prior research distinguishes between two different types of appraisal occurring concurrently: primary and secondary (Lazarus and

Folkman, 1984). In the context of received phishing warnings, the primary appraisal is when the user evaluates the threat posed by the event. During secondary appraisal, users determine which of the resources at their disposal could or would work to counteract the potential phishing attacks. These resources do not reflect individuals' actions per se, but rather the countermeasures available to them (Pearlin and Schooler, 1978). These two appraisal processes aid the individuals to adapt to the new situation (Lazarus and Folkman, 1984). Based on how serious the potential threat is appraised and what options the individual has to cope with it, specific adaptation strategies are revealed (Bala and Venkatesh, 2015; Stein et al., 2015). But the appraisals not only provide users' individual reasoning toward the appropriateness of specific adaptation strategies, they are also driving their motivation to protect themselves and their organization (Boss et al., 2015). In the security context, our understanding of the coping process, how users appraise an event, and how they adapt to the new situation is predominately based on protection motivation theory (PMT) (Boss et al., 2015; Crossler et al., 2013; Herath and Rao, 2009; Johnston and Warkentin, 2010; Lee and Larsen, 2009).

The majority of empirical studies in IS research in general and in behavioral IS security research in particular primarily focus on the relationship between the cognitive appraisals processes and the formation of protection motivation, as well as subsequent adaptive behaviors (Crossler et al., 2014). However, little is known about how individuals appraise a discrepant IT event, like security warnings for phishing, because the appraisals "*do not reveal why a particular cue is more or less salient for an individual user*" (Stein et al., 2015). This lack of understanding is grounded in the fact that extant research has largely omitted the antecedents of threats and coping appraisals, even though original PMT literature emphasizes the importance of the sources of information on which individuals base their assessment of the magnitude of threats and their abilities to address such threats (Milne et al., 2000).

In order to fill this research gap, this research introduces the awareness concept in the context of individuals' protection motivation by theorizing that security awareness shapes cognitive threat and coping appraisal processes. Unlike other research representing awareness as a monolithic construct, we differentiate two types of security-related awareness: threat awareness and countermeasure awareness, arguing that individuals are cognizant of different security threats and risks, and of countermeasures that could be used against such threats. We propose that understanding these two forms of awareness reveals what makes cues being salient for individual users (Stein et al., 2015). Thus, our research question is: *How do threat and countermeasure awareness shape IS users' threat and coping appraisals?*

We will address this research question using a multi-method experimental design including the use of eye tracking and face-reading software to capture users' awareness and their actual emotional fear of phishing attacks to monitor their response to fear appeals. Before describing the design of our field experiment, we will briefly introduce the theoretical background of our work and hypothesize the relationships in our research model.

In addition to our core contribution of how threat and countermeasure awareness shape individual threat and coping appraisal processes, this study will support further research on understanding users' protection motivation by providing a research model based on PMT that is tested through a manipulated fear appeal. Furthermore due to our experimental setting we can measure fear and actual security-related behaviors objectively based on facial recognition and eye-tracking data. For practice, we will provide an understanding on how to design electronically transmitted fear appeals that both raise awareness and motivate users' protective behaviors.

2 Theoretical Background – Core concepts

In order to contribute to current research, we aim to bridge the research gap how and under what circumstances threat and coping appraisals can be influenced in order to enhance users' protection motivation. Therefore, we introduce the underlying concepts – security awareness and fear appeals – in a first step and embed them in the theoretical basis of PMT in a second step.

2.1 Security Awareness

Security awareness – an individual's knowledge of particular security threats and potential countermeasures against those threats (Siponen, 2000; Thomson and Solms, 1998) – is still an underresearched phenomenon as an influencing factor for users' protection motivation. One notable exception is a study done by Posey et al. (2015), who argued that security education, training, and awareness (SETA) programs act as key distribution channel of fear appeals within organizations. Without considering security awareness per se, they found empirical support that the frequency of a SETA program helps to improve users' understanding of threat appraisal and coping appraisal process. Unfortunately based on their approach, the understanding of how information from external sources influences different appraisal processes is still rather limited as the authors measured the impact of the frequency of a SETA program participation just on a binary scale. Within behavioral IS security research, prior approaches analyze the direct and indirect impact of security awareness on security-related behaviors, such as coping with IS risk (Straub and Welke, 1998), IS misuse (D'Arcy et al., 2009; Hovav and D'Arcy, 2012), IS security policy compliance (Bulgurcu et al., 2010; Putri and Hovav, 2014), unauthorized information disclosure (Jenkins and Durcikova, 2013), and the use of security technologies (Dinev and Hu, 2007; Kumar et al., 2008).

Within this research we argue that security awareness is in fact a multidimensional variable. That is, on one hand individuals need to be aware of threats and on the other hand, they have to be aware of countermeasures that could be implemented against such threats (Siponen, 2000; Thomson and Solms, 1998). Following this, we define *threat awareness* as the degree to which users are cognizant of security threats, while *countermeasure awareness* refers to the degree to which users are cognizant of countermeasures that can eliminate or minimize these threats. Threat and countermeasure awareness shape the appraisals of coping and the related threat.

2.2 Fear Appeals and Protection Motivation Theory

A fear appeal is a stimulus designed to trigger fear as well as the threat appraisal and coping appraisal processes (Floyd et al., 2000; Maddux and Rogers, 1983; Milne et al., 2000). The fear appeal literature uses a message (i.e., fear appeal) as a manipulation. Only few IS security PMT-related studies actually incorporated fear appeals (Boss et al., 2015; Johnston et al., 2015; Johnston and Warkentin, 2010), even though the use of fear appeals is a fundamental cornerstone of PMT research (Floyd et al., 2000; Maddux and Rogers, 1983).

The focal theoretical concept underlying this research is PMT (Maddux and Rogers, 1983; Rogers, 1975). Originally rooted in coping and fear appeals literature, PMT is frequently used in behavioral IS security research to gain an understanding of an individual's decision to engage in security practices as a form of coping mechanism, such as taking measures to increase the security of home computers (Anderson and Agarwal, 2010), complying with information security policies at work (Herath and Rao, 2009), and adopting protective security technologies or services (Herath et al., 2014; Johnston and Warkentin, 2010; Lee and Larsen, 2009), among others.

According to PMT, *protection motivation* – the intention to protect oneself from a potential threat – is formed by two cognitive appraisal processes: threat appraisal and coping appraisal. Threat appraisal is based on *perceived threat vulnerability* (i.e., the belief that the threat applies to an individual), and *perceived threat severity* (i.e., the belief that the threat will cause consequential harm) (Maddux and Rogers, 1983). Once a threat is perceived, *Fear*, a negatively valenced emotion, occurs and inspires protection motivation (Floyd et al., 2000). Coping appraisal involves the belief that the recommended behavior will be effective in reducing the threat (i.e., *response efficacy*), that one can successfully enact the recommended behavior (i.e., *self-efficacy*), and the costs associated with the recommended behavior (i.e., *response costs*) (Maddux and Rogers, 1983).

3 Research Model and Hypotheses Development

As a theoretical basis for our research model (Figure 1), we use the core PMT nomology commonly applied in security-related PMT research (Boss et al., 2015), and extend it by adding the effect of fear appeals, and the introduction of two important new constructs: threat awareness and countermeasure awareness, representing important sources of information that are the basis for individuals' perceptions of threats and countermeasures (Maddux and Rogers, 1983; Milne et al., 2000). The model conceptualizes how the awareness constructs shape the threat appraisal and coping appraisal mechanisms. We refrain from hypothesizing the relationships between constructs of threat appraisal and protection motivation, and constructs of coping appraisal and protection motivation, because meta-analyses of applications to health-related behaviors (Floyd et al., 2000; Milne et al., 2000) and security-related behaviors (Sommestad et al., 2015) both support the notion that these PMT variables have a significant influence on protection motivation. Further support has been provided by empirical studies in the behavioral IS security domain that tested all constructs of the core PMT nomology (Boss et al., 2015). Thus, we choose not to replicate these established relationships within our research approach since it will not create new knowledge. Nevertheless, for reasons of theoretical and statistical comprehensiveness, we will provide empirical support for these relationships.

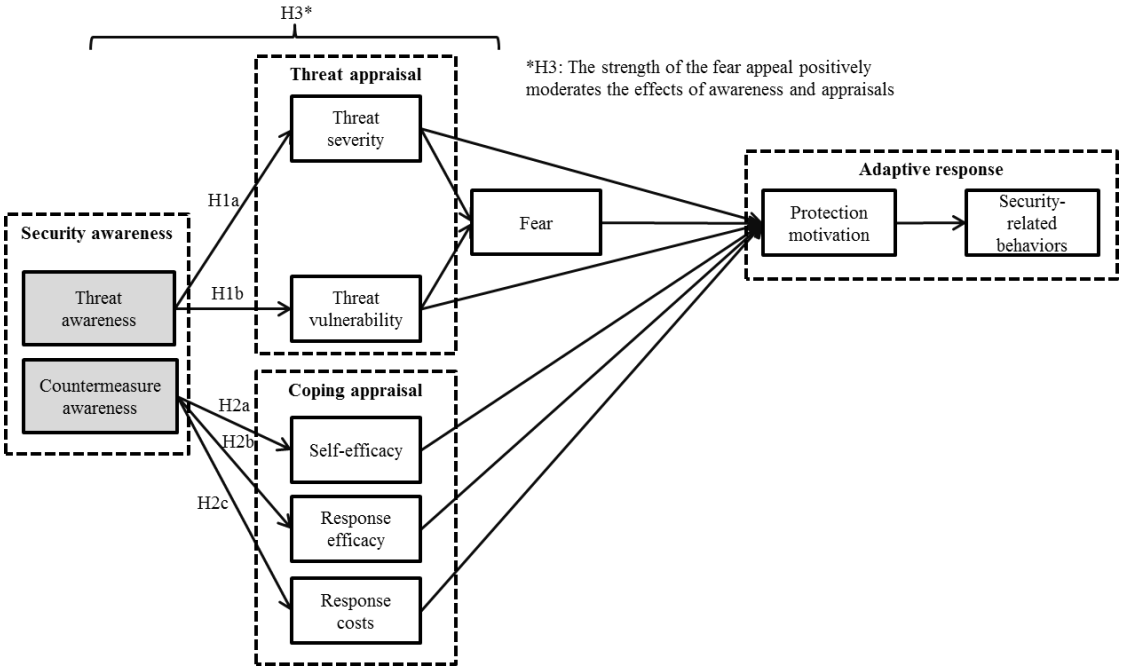

Figure 1. Research model

In phishing attacks and other schemes that rely on fake e-mails and websites, attackers use deception to lure their victims into complying with their request. The cognitive process of detecting deception entails noticing and interpreting inconsistent cues between the deceptive event, e.g. grammatical errors in a phishing e-mail, and users' past experiences, guided by cognitive heuristics (Johnson et al., 2001). Thus, threat awareness entails being aware of the tactics involved in deception, e.g. having the knowledge and understanding of how to spot phishing e-mails and spoof websites (Wang et al., 2012). Phishing attacks are an indication of anticipation that sensitive information will be gathered, identity theft will be committed, or access to data or funds will be gained.

Being more cognizant about the environment's current state of activity and threats should result in more accurate estimates about the risks associated with them (i.e., the severity of threats and the vulnerability towards these threats). However, individuals who are not aware of threats may underestimate the risks associated with them. At the same time, if individuals are aware of the presence of cer-

tain technical or procedural countermeasures, they should be more able to appraise whether they are capable of coping with the threat. In relation to phishing attacks, this implies that if users are more aware of available options to minimize or avoid a phishing threat, they should (1) feel more confident to take relevant actions to thwart phishing (i.e., self-efficacy), (2) perceive that they are effective in reducing the threat (i.e., response efficacy) as they convey the perception that their information assets would be secure if the countermeasures are in place, and (3) perceive that the costs (e.g. time and effort to execute what is needed to reduce the threat) are increased by these countermeasures (i.e., response costs). For instance, installing recommended anti-virus software may result in a regular update request that may interrupt users from their primary activities and increase physical and cognitive load (Bulgurcu et al., 2010; Putri and Hovav, 2014). Thus, threat awareness will have a positive effect on the related components of the threat appraisal process, i.e., perceived threat severity and perceived threat vulnerability, while countermeasure awareness will positively influence those in the coping appraisal process, i.e., response efficacy, self-efficacy, and response costs.

Hypothesis 1a/1b: Threat awareness positively impacts perceived severity of threats/perceived vulnerability of threats.

Hypothesis 2a/2b/2c: Countermeasure awareness positively impacts response efficacy/self-efficacy/response costs. .

In terms of the two awareness variables, we also assume that their effect will be enhanced by several context factors. Famous examples for such context factors in the IS security context are fear appeals. A fear appeal should ideally contain details of the threat itself (to convey the severity of the threat and the user's susceptibility to it) and of the measures that can be taken to avoid or to reduce its impact (to convey response efficacy and user's self-efficacy) (Anderson et al., 2016; Milne et al., 2000). An effective fear appeal drives the entire adaptive response (non-adaptive responses are outside the scope of the model; cf. (Maddux and Rogers, 1983; Witte, 1994). In behavioral IS security research, few studies manipulated an actual fear appeal (Boss et al., 2015; Johnston et al., 2015; Johnston and Warkentin, 2010). In the context of data backups and coping with malware, Boss et al. (2015) found full support for the core PMT model when high-fear appeal manipulations were used, i.e., high-fear appeal manipulations evoked more fear and supporting threat, which in turn increased protection motivation and subsequent behaviors, than do low-fear appeal manipulations. In addition, a high-fear appeal should also improve users' propensity to notice and attribute a threat, thus increase their threat awareness. More specifically, it should facilitate individuals' cognitive process in arousing suspicion about inconsistencies between the cues manipulated in e-mails or websites and the truth, generating and evaluating hypotheses on the situation, and reaching a conclusion about whether there is deception in an e-mail or website (Johnson et al., 2001; Zahedi et al., 2015). At the same time, it should communicate existing technical and procedural countermeasures available to the user, thus increasing their countermeasure awareness. Users need to become aware of a manageable path forward that provide appropriate direction and support. Therefore, stated in broad terms:

H3: The higher the fear-appeal, the stronger all relationships between awareness and appraisals.

4 Research Methodology

To empirically test our research model, we conducted a multi-method approach consisting of a field experiment using eye tracker technology together with a post-experimental survey. In the following, we will (1) provide details on the tasks and fear-appeal manipulations; (2) describe our experimental setup and data collection methods; (3) explain our measures; and (4) describe our next steps.

4.1 Tasks and Fear-Appeal Manipulations

The participants are informed that the experiment's goal is to study viewing behavior while processing e-mails and browsing on websites. The whole experiment takes about 60 minutes. Participants are

given an e-tray exercise, in which they take the role of an employee at a fictional company and are required to read and process 20 e-mails. For tasks within e-mails that prompt to access a website with usernames and passwords, accounts belonging to the university are provided. The participants are explicitly prompted to treat such information "as if they were their own" and are instructed to keep them confidential. These instructions are intended to make our data appear worthy of protection without overly emphasizing information security itself. The set of e-mails consists of legitimate e-mails leading to legitimate websites and of real-world phishing examples in which URL links to websites are fraudulent and aim to lure individuals into submitting personal information or downloading files.

We use a low and a high fear appeal to manipulate participants' motivation to protect themselves from phishing attacks. Participants are assigned to two groups based on which appeal they received, which is dependent on their own behavior during the experiment. Participants in the low fear-appeal condition have read one single message warning of the threat of phishing and recommending countermeasures against it as part of an e-mail sent by the company's IT department. Participants in the high fear-appeal condition received a red security warning banner branding a site they have tried to access as deceptive, describing threats related to the site and offering different options on how to cope with it.

4.2 Experimental Setup and Data Collection Methods

Collecting the eye tracking and facial expression data requires a meticulous technical design. The experimental setup consists of four main components: the eye tracker, the web client, the webserver with experiment-specific web content, and a web cam. The four components are applied as follows.

First, we use Tobi Pro X2-30 eye tracker, which is a small device attached to the bottom of the screen (a 19" LCD monitor in our case) and designed to capture data at 30 Hz. The eye tracker is calibrated individually for each user. During the experiment, all screen activities are recorded for analysis by using Tobii Pro Studio eye tracking software (Tobii, 2016), which tracks the participants' eye fixations, saccades, and pupil dilation during the entire experiment. Second, the web client runs on a personal computer with Windows 7 and all participants use the same browser to ensure that the types of visible security indicators are identical for all users. Third, while participants are able to access pages normally for links in non-phishing emails, links from phishing emails lead to phishing websites hosted on our webserver. These pages mirror regular pages and allow the entry of logins of the fictional user data provided for the experiment. This enables us to collect report data on clicks on links in e-mails, and especially valid submissions of account data (i.e., successful phishing attacks). Fourth, we capture participants' facial expressions during the experiment by using a Logitech HD Pro Webcam C920 with Full HD 1080p. We use FaceReader 7 (Noldus, 2016) for facial analysis to capture participants' actual fear and control for the effectiveness of our treatment fear appeal. By objectively measuring fear as it occurs, we will be able to mitigate challenges of self-report measures of fear (Anderson et al., 2016). Figure 2 illustrates Face Reader's analysis visualization consisting of the automatic mapping of an artificial face model describing the location of over 500 key points and the texture of the face. The output of the emotion fear facially expressed by a participant in response to the high fear appeal is based on the action units of the Facial Action Coding System (Ekman and Friesen, 1977). On the right side of Figure 2, participants' eye fixations while reading the fear appeal are visualized.

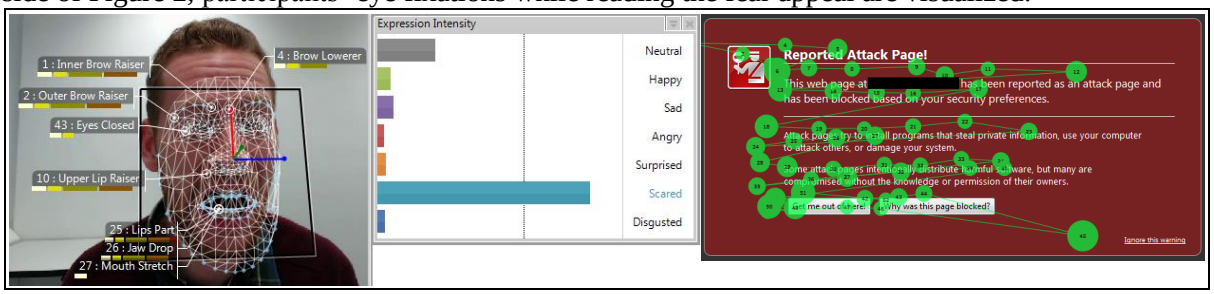

Figure 2. FaceReader Analysis Visualization for the Emotional Expression of Fear and Tobii Analysis Visualization for Eye Fixations

The post-experimental survey part in our research design takes individual differences (e.g., age, gender, personality traits), security-related IS knowledge, prior experience with phishing, and the measures related to the PMT core constructs into account.

4.3 Measures

The measures on the PMT core constructs within this work have been adopted from prior PMT literature (Milne et al., 2002) and modified to assess the constructs described in the research model in the context of phishing using 7-point Likert-type scales. Additionally, by using eye tracking software, we are able to measure participants' behaviors and awareness based on objective data. Posey et al. (2013) provide a basis for coding protection-motivated behaviors to this extent, particularly legitimate e-mail handling and secure software, e-mail, and Internet use, which we will complement with behavioral reactions to phishing e-mails from earlier work (Sheng et al., 2010). The behaviors are structured in security-related behaviors in the e-mail program, the browser window, and the system hard drive. The more actions fulfilled in the respective category the higher the security-related behavior to avoid or to allow security-related threats. To measure participants' security awareness we have self-developed two constructs: threat awareness and countermeasure awareness. First, threat awareness is reflected in participants' collection process of security and deception cues in e-mail and on websites. This includes looking for the e-mail source, title/subject line, design of link URLs, unusual additions to the URL of the website, SSL certificate, secure https connections, among others (Dhamija et al., 2006; Pfeiffer et al., 2014; Whalen and Inkpen, 2005). Second, countermeasure awareness is reflected in participants' collection process of cues from countermeasures. This includes looking for the presence and status reports of fake-website detection tools (Zahedi et al., 2015), anti-spyware tools (Boss et al., 2015), anti-virus scanner and firewall software (Anderson and Agarwal, 2010). Threat awareness and countermeasure awareness are measured based on participants' number of fixations on areas of interest (Rayner, 1998) in e-mails and on the browsed websites. These areas of interest depict the deception and security cues described above. On average individuals can process all information from a fixation in about 200-500 ms. The more cues are fixated for more than 200 ms, the higher the respective awareness of the participant. To measure participants' fear of phishing, we filmed their facial expressions during the experiment. Based on the facial analysis by the FaceReader software, we are able to distinguish the emotions expressed facially in reaction to the e-mails received in the experiment and whether the infected phishing e-mails and security warnings cause an emotion of fear. FaceReader's metrical output of expression intensity describes the emotion as a value ranging from 0 to 1 and considers the emotion with the maximum value as the dominant one and using a threshold value of it being active for 0.5 seconds. FaceReader's robustness and reliability was tested in several studies highlighting that the software corresponds with the evaluations of trained observers in up to 69%-89% of all cases (Lewinski et al., 2014; Terzis et al., 2010). We double-check the results of the FaceReader software by also asking participants in the post-experimental survey if they were scared of phishing e-mails during the experiment (Boss et al., 2015). We use the results to control for the effectiveness of our fear appeal manipulation. If fear appeal manipulation is successful, elements of threat appraisal, fear, and actual security-related behavior as suggested by the fear appeal message should be affected.

4.4 Demographics of the Experiment Participants

Primary data has so far been collected from experiments with 107 employees in organizations of various sectors, including financial services (n = 57), education (n = 24), manufacturing (n = 7), government (n = 4), energy (n = 3), retail (n = 2), and other (n = 8). Participation was voluntary and anonymous and the employees were told that the purpose of the experiment is academic research and that independent university scholars would conduct the experiment and analyze the results. Table 1 presents demographic information of the employees. These employees use a computer at work for 6.55 hours per day on average (SD 2.41), and own an average of 3.36 email accounts (SD 2.42).

Gender		**Age**		**Highest level of education**		**Career status**	
Male	54.2%	< 20	1.9%	Less than high school degree	20.6%	Trainee	0.9%
Female	45.8%	20-29	8.4%	High School degree or similar	22.4%	(Administrative) clerk	40.2%
		30-39	26.2%	Bachelor degree or similar	5.6%	Young professional	5.6%
		40-49	28.0%	Master degree or similar	46.7%	Professional	39.3%
		50-59	21.5%	Doctorate degree	1.9%	Manager	7.5%
		60-69	4.7%	Other	2.8%	Other	5.5%
		n.s.	9.3%				

Table 1. Demographic information of the participants (n=107)

5 Next Steps

As of now, we are not finished with data collection. In the meantime, we define areas of interest for subsequent analysis of our gaze data, particularly to compute the mean number of fixations in the areas of interest, using Tobii Pro Studio eyetracking software. Simultaneously, we code participants' security-related behaviors as described in the previous section. Further, for evaluating facial expressions we use FaceReader 7 software to analyze objectively expressed fear before, during, and after the high fear or low fear appeal stimulus. After these three steps are achieved we will combine objective data (eye fixation data, the facially expressed emotion of fear, and actual security behaviors) and subjective perceptual data (users' beliefs, cognitions, and intentions) to analyze our overall research model and to test the hypotheses quantitatively.

When interpreting our results some initial limitations need to be considered. First, realism is a key concern of an experiment approach and we designed the scenario as realistic and contextually relevant as possible. However, since participants' behaviour was recorded, we need to address the issue that participant's browsing behaviour in the experiment may differ from natural browsing behaviour. Another limitation is the use of only one context, namely phishing. In addition to looking at attacks from outside the company, future research could examine other contexts of behavioral security, such as threats coming from inside the company to identify additional areas of improvement. It remains to be seen how the proposed relationships in our model change in the context of such insider threats.

References

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D. and Jeffrey L. Jenkins (2016). "How users perceive and respond to security messages: A NeuroIS research agenda and empirical study." *European Journal of Information Systems* 25 (4), 364–390.

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

Bala, H. and Viswanath Venkatesh (2015). "Adaptation to Information Technology: A Holistic Nomological Network from Implementation to Job Outcomes." *Management Science* 62 (1), 156–179.

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

Bulgurcu, B., Cavusoglu, H. and Izak Benbasat (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." *MIS Quarterly* 34 (3), 523–548.

Carver, C. S. and Michael F. Scheier (1994). "Situational coping and coping dispositions in a stressful transaction." *Journal of Personality and Social Psychology* 66 (1), 184–195.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Richard Baskerville (2013). "Future directions for behavioral information security research." *Computers & Security* 32, 90–101.

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

D'Arcy, J., Hovav, A. and Dennis Galletta (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research* 20 (1), 79–98.

De Guinea, A. O. de and J. Webster (2013). "An Investigation of Information Systems Use Patterns: Technological Events as Triggers, the Effect of Time, and Consequences for Performance." *MIS Quarterly* 37 (4), 1165–1188.

Dhamija, R., Tygar, J. D. and M. Hearst (2006). "Why phishing works." In: *Proceedings of the SIGCHI Conference 2006*: ACM.

Dinev, T. and Qing Hu (2007). "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies." *Journal of the Association for Information Systems* 8 (7), 386–408.

Ekman, P. and Wallace V. Friesen (1977). *Manual for the facial action coding system*. Palo Alto, CA: Consulting Psychologists Press.

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

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

Herath, T. and H. Raghav Rao (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." *European Journal of Information Systems* 18 (2), 106–125.

Hovav, A. and John D'Arcy (2012). "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea." *Information & Management* 49 (2), 99–110.

Jenkins, J. L. and A. Durcikova (2013). "What, I Shouldn't Have Done That?: The Influence of Training and Just-in-Time Reminders on Secure Behavior." In: *Proceedings of the 34th International Conference on Information Systems (ICIS 2013)*. Milan, Italy.

Johnson, P. E., Grazioli, S., Jamal, K. and R. Glen Berryman (2001). "Detecting deception: adversarial problem solving in a low base-rate world." *Cognitive Science* 25 (3), 355–392.

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

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

Kumar, N., Mohan, K. and Richard Holowczak (2008). "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls." *Decision Support Systems* 46 (1), 254–264.

Lazarus, R. S. and Susan Folkman (1984). *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Lee, Y. and Kai R. Larsen (2009). "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software." *European Journal of Information Systems* 18 (2), 177–187.

Lewinski, P., den Uyl, T. M. and Crystal Butler (2014). "Automated facial coding: Validation of basic emotions and FACS AUs in FaceReader." *Journal of Neuroscience, Psychology, and Economics* 7 (4), 227.

Louis, M. R. and R. I. Sutton (1991). "Switching Cognitive Gears: From Habits of Mind to Active Thinking." *Human Relations* 44 (1), 55–76.

Maddux, J. E. and Ronald W. Rogers (1983). "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change." *Journal of Experimental Social Psychology* 19 (5), 469–479.

Milne, S., Orbell, S. and Paschal Sheeran (2002). "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions." *British Journal of Health Psychology* 7 (2), 163–184.

Milne, S., Sheeran, P. and Sheina Orbell (2000). "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory." *Journal of Applied Social Psychology* 30 (1), 106–143.

Noldus (2016). *FaceReader: Tool for automatic analysis of facial expression: Version 7*. Wageningen, the Netherlands: Noldus Information Technology B.V.

Pearlin, L. I. and Carmi Schooler (1978). "The Structure of Coping." *Journal of Health and Social Behavior* 19 (1), 2–21.

Pfeiffer, T., Kauer, M. and J. Röth (2014). "A Bank Would Never Write That! - A Qualitative Study on E-Mail Trust Decisions." In: *Informatik 2014 Big Data - Komplexitaet meistern*. Berlin, Heidelberg: Springer-Verlag.

Posey, C., Roberts, T., Lowry, P. B., Bennett, B. and James Courtney (2013). "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors." *MIS Quarterly* 37 (4), 1189–1210.

Posey, C., Roberts, T. L. and Paul Benjamin Lowry (2015). "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets." *Journal of Management Information Systems* 32 (4), 179–214.

Putri, F. F. and Anat Hovav (2014). "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory." In: *Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*. Tel Aviv, Israel.

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

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change1." *The Journal of Psychology* 91 (1), 93–114.

Sheng, S., Holbrook, Mandy, Kumaraguru, P., Cranor, L. F. and Julie Downs (2010). "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atlanta, Georgia, USA: ACM.

Siponen, M. T. (2000). "A conceptual foundation for organizational information security awareness." *Information Management & Computer Security* 8 (1), 31–41.

Sommestad, T., Karlzén, H. and Jonas Hallberg (2015). "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour." *International Journal of Information Security and Privacy* 9 (1), 26–46.

Stein, M.-K., Newell, S., Wagner, E. L. and Robert D. Galliers (2015). "Coping with information technology: mixed emotions, vacillation, and nonconforming use patterns." *MIS Quarterly* 39 (2), 367–392.

Straub, D. W. and Richard J. Welke (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly* 22 (4), 441–469.

Terzis, V., Moridis, C. N. and A. A. Economides (2010). "Measuring instant emotions during a self-assessment test." In: *Proceedings of the 7th International Conference on Methods and Techniques in Behavioral Research: The use of FaceReader*. ACM.

Thomson, M. E. and Rossouw von Solms (1998). "Information security awareness: educating your users effectively." *Information Management & Computer Security* 6 (4), 167–173.

Tobii (2016). *Tobii Pro Studio Version 3.4*. Stockholm, Sweden: Tobii AB (publ).

Tyre, M. J. and Wanda J. Orlikowski (1994). "Windows of Opportunity: Temporal Patterns of Technological Adaptation in Organizations." *Organization Science* 5 (1), 98–118.

Wang, J., Herath, T., Chen, R., Vishwanath, A. and H. Raghav Rao (2012). "Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email." *IEEE Transactions on Professional Communication* 55 (4), 345–362.

Whalen, T. and Kori M. Inkpen (2005). "Gathering evidence: use of visual security cues in web browsers." In: *Proceedings of Graphics Interface 2005*: Canadian Human-Computer Communications Society.

Witte, K. (1994). "Fear control and danger control: A test of the extended parallel process model (EPPM)." *Communications Monographs* 61 (2), 113–134.

Zahedi, F., Abbasi, A. and Yan Chen (2015). "Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance." *Journal of the Association for Information Systems* 16 (6), 448–484.