Journal of Management Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/mmis20

The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security

Sebastian W. Schuetz , Paul Benjamin Lowry , Daniel A. Pienta & Jason Bennett Thatcher

To cite this article: Sebastian W. Schuetz , Paul Benjamin Lowry , Daniel A. Pienta & Jason Bennett Thatcher (2020) The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security, Journal of Management Information Systems, 37:3, 723-757, DOI: 10.1080/07421222.2020.1790187

To link to this article: https://doi.org/10.1080/07421222.2020.1790187

JOURNAL OF MANAGEMENT INFORMATION SYSTEMS
2020, VOL. 37, NO. 3, 723–757
https://doi.org/10.1080/07421222.2020.1790187

Routledge
Taylor & Francis Group

Effectiveness of Abstract versus Concrete Fear Appeals in Information Security

Sebastian W. Schuetz[a], Paul Benjamin Lowry[b], Daniel A. Pienta[c], and Jason Bennett Thatcher[d]

[a]Department of Information Systems and Business Analytics, College of Business, Florida International University, Miami, FL, USA; [b]Department of Business Information Technology, Pamplin College of Business, Virginia Tech, Blacksburg, VA, USA; [c]Hankamer School of Business, Baylor University, Waco, TX, USA; [d]Department of Management Information Systems, Temple University, Philadelphia, PA, USA

ABSTRACT

Information security (ISec) is a pervasive concern of individuals, organizations, and governments. To encourage individuals to engage in and learn about secure behaviors, ISec research has turned to fear appeals, which are short messages that communicate threats and efficacy to elicit protection motivation among recipients. ISec research has reported contradictory findings on what makes fear appeals effective in ISec contexts, and this lack of clarity is problematic, because it may lead to incorrect conclusions. For example, some studies have argued that the mixed findings arise from differences between personal and organizational contexts and that fear appeals do not work well among organizational users. However, this argument has not been empirically tested, and differences in message design provide an equally plausible explanation, which has also not been tested. To reconcile the mixed findings across these studies, we test the effects of *context* (i.e., personal users vs. organizational users) and degree of *message abstractness* (i.e., abstract vs. concrete) on fear-appeal outcomes. We draw from construal-level theory to conceptualize the differences between abstract and concrete fear appeals. Across three experiments, we find evidence that concrete fear appeals are more effective than abstract fear appeals for the purpose of stimulating fear-appeal outcomes. Furthermore, by comparing two identical experiments—one conducted with personal users and another conducted with organizational users—we find differences in participants' responses to fear appeals. However, contrary to our expectations, our findings suggest that organizational users report higher levels of fear and protection motivation than personal users. This finding is not a theoretical contradiction: the theoretical crux of an effective fear appeal is that it must be personally relevant to stimulate fear; correspondingly, we show that concrete fear appeals help stimulate fear and the desired protective response. Moreover, concrete fear appeals increase actual compliance behaviors, not just intentions. Thus, our findings suggest that the mixed findings in the literature may be a product of message abstractness and differences among audiences. This has pivotal implications for how to construct fear appeals in research and practice.

KEYWORDS

Information security threats; fear appeals; protection motivation theory; construal-level theory; cybersecurity; secure behaviors

CONTACT Paul Benjamin Lowry Paul.Lowry.PhD@gmail.com Department of Business Information Technology, Pamplin College of Business, Virginia Tech, Pamplin Hall, Suite 1007, 880 West Campus Drive, Blacksburg, VA 24061 USA.

Supplemental data for this article can be accessed on the publisher's website

Introduction

Fear appeals have emerged as a key tool to improve information security (ISec). *Fear appeals* communicate a combination of threat and efficacy as a means of evoking positive changes in behavior [81, 105]. Originally developed in the healthcare literature, they use personally relevant threats such as AIDS [e.g., 22] or lung cancer [e.g., 21] to promote health-protective behaviors. Due to the efficacy of fear appeals in health research, ISec scholars have examined their capacity to encourage ISec-relevant behaviors, such as compliance with ISec policies [e.g., 9, 20, 50].

However, the ISec literature is replete with mixed findings on the efficacy of fear appeals [98]. Despite their common use of protection motivation theory (PMT), ISec studies have reported contradictory evidence on *every* predictor of fear-appeal effectiveness. Whereas the original healthcare literature established, via multiple meta-analytical studies, that threats and fear are key determinants of fear-appeal outcomes regardless of the theory involved [27, 81, 105], only some ISec studies confirm these relationships [e.g., 9, 64]. Other ISec studies report contradictory evidence that cast doubt on whether ISec fear appeals should focus on threats and fear [47, 50, 101]. Given these mixed findings, it is unclear how to design effective fear appeals for an ISec context.

One possible explanation for these mixed findings is the subtle differences between the user contexts of studies [48, 50, 101]. Some studies apply fear appeals to *personal users*, using ISec threats that target personal assets, others apply them to *organizational users (i.e., employees)*, using threats that target organizational information assets. The logic here is that because organizational assets are of less personal relevance to individual employees, organizational ISec threats will be seen as less personally relevant [48, 50, 66, 101] and will thus be less likely to deliver a personally relevant threat that generates fear [101]. However, this explanation has not been validated because researchers have not compared fear generation among personal users versus organizational users in the same study. Whether context can account for the mixed findings of ISec fear-appeals studies thus remains an open question.

Further explanations may help to untangle the mixed findings. In this paper, we also investigate *message abstractness*, which is the extent to which fear appeals are abstract or concrete. *Abstract fear appeals* are messages that are more generic and thus describe threats and responses in a high-level fashion (e.g., "*victims* need to put forth substantial *effort* to recover from spear-phishing attacks"), whereas *concrete fear appeals* are specific and describe threats and responses with rich detail and examples (e.g., "*you* will need to *employ lawyers* to recover from spear-phishing attacks"). The degree of message abstractness used by ISec studies varies considerably, which may determine whether a threat is personally relevant enough to generate fear. Whereas some ISec studies have relied on concrete fear appeals [e.g. 9, 64], the majority of studies present threats more generally or abstractly [e.g. 50, 66, 101]. Regarding fear appeals, heterogeneity in message abstractness may be problematic, because it may cause divergent findings and impede the development of a cumulative understanding of how fear appeals motivate ISec behavior [107]. It is also unclear which fear-appeal type is more effective; thus, examining the role of message abstractness may offer a clearer explanation of the mixed findings.

To understand whether message abstractness or context can explain the mixed findings, we ask, *What are the effects of message abstractness and user context on fear-appeal*

outcomes? To conceptualize message abstractness, we draw from construal-level theory (CLT) to craft abstract and concrete fear appeals. To explore the effects of message abstractness and context, we conduct three field experiments using samples drawn from personal and organizational users. Study 1 sampled personal users as participants, and Study 2 sampled employees as participants. Thus, our research is the first to test the effect of a single fear appeal among two different populations. Study 3 then retests our hypotheses using a distinct set of manipulations, which provides further evidence for the robustness of our findings.

Background on fear appeals and construals

Fear appeals and protection motivation theory (PMT)

Fear appeals were developed as an intervention to stimulate positive behavioral change among large audiences in health-communication contexts (e.g., smoking cessation, weight loss). These behavioral interventions, based on threat and efficacy messages, have been frequently studied in the context of public service announcements and health communication [22, 95, 105-107]. Similarly, fear appeals have frequently been studied in ISec research to understand how to motivate more secure behaviors among personal users and employees [e.g., 9, 50, 66, 98]. Scholars have developed several theories to explain *what* makes fear appeals effective. In ISec research, PMT [80, 81] is the primary theoretical foundation for studies that have applied fear appeals to promote ISec [98].

To explain fear-appeal effectiveness, PMT suggests that fear-inducing communications from threat and efficacy (i.e., *fear appeals*) trigger a sequence of cognitive appraisal processes that predict protection motivation. The first process is the *threat appraisal process*, which evaluates *threat severity perceptions* (i.e., recipients' beliefs that an ISec threat is serious and potentially severe) and *perceived threat vulnerability* (i.e., recipients' expectations that they will be susceptible to a particular threat) [83]. Crucially, PMT explains that people must consider the threat to be *personally relevant* to be effective, which can lead to protection motivation, but only if the recipients have adequate coping mechanisms [27, 82]. PMT originally downplayed the role of fear in fear appeals [80, 81], but it emerged as a factor in later versions [9, 27, 82], as fear emerged as increasingly fundamental in other competing theories [cf. 105, 106, 107]. Several meta-analyses across broader fear-appeals research support fear's ability to shape motivation and have found that it mediates the relationship between threats and protective motivation [e.g., 27, 94, 95, 107]. Likewise, ISec researchers have treated fear as a mediator between threat perceptions and protection motivation. However, this has only been done in studies that used fear appeals in personal security contexts [9]; it has yet to be fully tested in an organizational ISec setting. The threat appraisal process also involves perceptions of *maladaptive rewards*, which are rewards gained from not mitigating the suggested threat, such as not complying with the recommendation conveyed by the fear appeal [27].

Subsequent to the threat appraisal process is the *coping appraisal process*, which evaluates the recommended coping response (suggested options for protecting against the threat) and one's ability to execute the response. The recommended coping response is evaluated in terms of its *response efficacy* (i.e., recipients' belief in the

Table 1. Conflicting evidence in ISec fear-appeal research.

	Supporting Evidence		Contradicting Evidence	
PMT Constructs	Personal	Organizational	Personal	Organizational
Threat severity	[6, 9] *[17]	[50, 101] *[34] *†[77] *[10] *[36]	[9, 66]	*[49] *[67] *[8]
Threat vulnerability	[6] *[17]	*[49] *[36]	[9, 66]	[50, 101] *[67] *[34] *[8]
Fear	[9]	n/a	n/a	[101] *[77] *[10]
Maladaptive rewards	[64]	*[77] *[10]	[9]	*[67]
Response efficacy	[66]	[47, 50, 101] *[34] *[77] *[10]	[9, 64]	*[49] *[36] *[8]
Self-efficacy	*[17]	[47, 50, 101] *[34] *[36]	[9, 64, 66]	*[49] *[67] *[8]
Response costs	[9]	*[67] *[34] *†[77] *[10]	[64]	*[49] *[8]

Notes: PMT, protection motivation theory. * Studies that did not use fear appeal manipulations to test their PMT-based theories. † Supporting evidence reported only for employees with high organizational commitment.

efficacy of the protective action) in conjunction with *self-efficacy* (i.e., their perceived ability to actually perform the protective action) versus *response costs* (i.e., all costs or expected costs that arise from carrying out the protective response) [27]. PMT predicts that recipients will engage in recommended protective responses only if the noxiousness of the threat outweighs the associated maladaptive rewards and only if the recommended coping response is perceived as executable, efficient, and affordable [9, 27, 62]. Crucially, what this means is that the threat and subsequent fear are just one part of an effective fear appeal; a fear appeal should ideally also increase one's sense of efficacy to cope with the threat and fear; if not, too much fear with too little efficacy can cause a maladaptive response instead of protection motivation [9]. Table 1 details all the potential constructs of PMT and Supplemental Online Appendix Figure 1.1 depicts them in a nomological network of constructs.

Mixed findings in ISec fear-appeal research

Despite several years of ISec research on fear appeals [9, 48], researchers are still working toward a cumulative body of knowledge [98] because studies report contradictory findings (see Table 1). Even though these studies share a foundation in PMT, conflicting findings exist for every core construct in PMT's nomological network of constructs. Some studies have found that protection motivation is driven by threat severity [e.g., 6, 9, 50], others have not [e.g., 49, 66, 67], some have found that protection motivation is driven by response efficacy [e.g., 47, 50, 66], and others have reported contradictory findings [e.g., 9, 49, 64]. These examples illustrate that the extant ISec research is unclear about the factors that drive protection motivation.

Two potential explanations can help unravel these mixed findings. One explanation is that these studies were conducted in different contexts [48, 50, 101]. This explanation suggests that whereas security threats in personal contexts have personally relevant consequences (i.e., loss of personal data), ISec threats in organizational contexts are organizationally relevant (i.e., loss of organizational data) but lack personal relevance and thus are surmised to be less effective with organizational users [48, 50, 101]. However, this hypothesis has not been validated, because no study has compared the efficacy of a single fear appeal on personal versus organizational users.

Furthermore, studies conducted in the same context sometimes report contradictory evidence. Although some studies have found that threat severity drives protection motivation in organizational contexts [50, 101], studies conducted in an organizational setting

have not found such evidence [49, 67]. Analogously, mixed findings have also been reported among studies conducted in a personal context [e.g., 6, 9, 64, 66]. Another intriguing finding is that employees with higher organizational commitment experience higher levels of threat, efficacy, and protection motivation than those with less commitment—implying that organizational ISec threats have the potential to be important and relevant to some employees [77]. However, the same study did not actually deliver manipulated fear appeals to employees to determine whether such a manipulation could increase the personal relevance of the appeals.

A second explanation is related to fear-appeal manipulations. Few ISec studies have actually delivered fear-appeal treatments in their research designs; worse, some researchers miss the point that a fear appeal should deliver both threat and efficacy, and instead only deliver threat, which can backfire. This is problematic, because PMT is, by definition, a theory that explains individuals' responses to fear appeals to predict when they are effective [80, 81]. However, as Table 1 shows, there are mixed findings even between studies that applied fear appeals to personal users. For example, one paper [66] found that response efficacy is a significant predictor of protection motivation, whereas others [9, 64] reported findings that suggest that self-efficacy is more important. One study [64] found that maladaptive rewards drive protection motivation, whereas another [9] found that maladaptive rewards are insignificant. Clearly, simply considering whether fear appeals were delivered does not lead to a sufficient explanation of the mixed findings.

We posit an alternative, more nuanced explanation of why these fear-appeal manipulations differ. The results of fear-appeal applications can differ dramatically depending on whether the fear appeals delivered (both in raising threat and efficacy) are *weak* or *strong* [9]. Although the broader fear-appeals literature [9, 27, 95, 105] has concluded that strong fear appeals are those that succeed in raising threat, fear, efficacy, and ultimately protection motivation, what makes fear appeals "strong" or effective is not well understood. Furthermore, most ISec studies have not actually measured fear outcomes (see Supplemental Online Appendix 1 Table 1.1). The problem is that a researcher can only know if a threat is personally relevant if it raises fear [9]. Moreover, in our review, we observed that studies lacked consistency in how they presented threats and responses in their fear appeals (Table A1). Thus, researchers cannot evaluate whether the mixed findings are due to the delivery of weak or strong fear appeals. Some studies used *concrete* language in their fear appeals (e.g., "the damages of data loss can amount to thousands of dollars" or "malware will make your computer inoperable"), whereas others employed *abstract* language (e.g., "data loss can have financial consequences" or "malware can harm your computer").

Crucially, in our review, a pattern emerged that suggests that *concrete* messages may be more effective than *abstract* messages in delivering personally relevant threats that elicit fear. This is evident in Supplemental Online Table 1.1: All studies reporting positive fear responses used *concrete* fear appeals, whereas the only study reporting negative fear responses used *abstract* fear appeals. If message abstractness does, in fact, determine whether fear appeals are weak or strong—due to the degree to which they are personally relevant—message abstractness is likely a key factor that can explain the mixed findings in the literature and can guide ISec research toward building more effective messages. Consequently, our research is driven by this compelling opportunity to determine whether

the mixed findings in the literature can be readily explained by differences in message abstractness.

Construal-level theory (CLT)

We leverage CLT to conceptualize message abstractness. CLT[1] is a psychological theory that explains how individuals mentally represent distant objects, actions, and events. The mental representations of these objects, actions, and events are called *construals* [26, 90]. CLT suggests that construals can differ in their degree of abstractness. For example, an abstract representation of an event could be "phishing attack," whereas a more concrete representation could be "phishing email from WellsFargo." Because CLT describes how abstract construals differ from concrete construals, we use CLT as a conceptual foundation to explain how abstract fear appeals differ from concrete ones. Fear appeals are like construals in that they represent threat events and coping actions but do so in the form of a persuasive message. However, the conceptual differences between abstract and concrete construals are still useful for conceptualizing the differences between abstract and concrete messages, because as respondents read a message, they will make a mental representation of it in a corresponding abstract/concrete form. Persuasion researchers have applied CLT to justify how users conceptualize differences in messages [e.g., 29, 53, 69]. Thus, we follow this research to conceptualize message abstractness based on different construals, per CLT.

CLT suggests that abstract construals differ from concrete construals in their features and their associated psychological distance (Table 2). First, abstract construals are more generic and schematic than concrete construals, which are more specific and detailed [26, 90]. *Abstract construals* describe events or actions with high-level features, whereas *concrete construals* use low-level features [96].[2] Abstract construals have fewer features than concrete construals, because abstract construals omit incidental details and focus on the central features of what they represent, whereas concrete construals provide incidental, more peripheral details of what they represent [26, 90]. We posit that such incidental details can make a crucial difference in conveying the necessary personal relevance of an effective fear appeal.

CLT suggests that abstract construals are useful for judging the desirability of what is represented, whereas concrete construals are useful for judging the feasibility of what is represented [4, 96]. The high-level features of abstract construals thus help individuals assess *why* an event or action should be sought or avoided, whereas the low-level features of concrete construals help individuals assess *how* these events can be avoided. Thus, feasibility appraisals entail judgments related to coping and efficacy.[3] Accordingly, in

Table 2. Conceptualizing message abstractness based on CLT.

Dimensions	Definition	Abstract	Concrete
Features	The degree to which descriptions are generic or specific	***Generic*** (e.g., phishing is dangerous); Focus on desirability (i.e., why)	***Specific*** (e.g., phishing asks for your credit card information); Focus on feasibility (i.e., how)
Psychological distance	The degree to which an event/action is depicted as being close or far away	***Distal*** (i.e., in the future, far away, others, hypothetical)	***Proximate*** (i.e., now, here, self, realistic)

Notes: CLT, construal-level theory.

contrast to the features of abstract construals, which are more *generic* and focus on *desirability*, the features of concrete construals are more *specific* and focus on *feasibility*. The latter should thus be more effective in strengthening both the personal relevance of a threat and the subsequent efficacy.

CLT further suggests that abstract and concrete construals are associated with *psychological distance* [57, 92, 96], which is the degree to which an event or action is perceived as close or far away [96]. For example, a spear phishing attack could be perceived as a *distal event* (i.e., in the distant future) or a *proximate event* (i.e., very soon). When events or actions are seen as distal, according to CLT, they are associated with abstract mental representations; when they are perceived as proximate, they are associated with concrete mental representations. That is, events or actions that are psychologically distal (e.g., in the future) evoke a judgment of desirability (e.g., "*why* should *someone* avoid phishing attacks *three months from now*?"), whereas construals that are psychologically close (e.g., now) evoke a judgment of feasibility (e.g., "*how* can *I* avoid a phishing attack *right now*?").

CLT explains that psychological distance has four dimensions: *temporal* (i.e., now vs. in the distant future), *spatial* (i.e., here vs. far away), *social* (i.e., me vs. others), and *hypothetical* (i.e., realistic vs. hypothetical). A construal is perceived as psychologically proximate if it is seen as present in the *here* (spatial) and *now* (temporal) and if one feels that it *realistically* (hypothetical) involves *oneself* (social). A construal is perceived as distant if it is located *in the future, in another place*, involves *others*, or occurs *hypothetically*.

CLT also explains that there is a bidirectional association between features and psychological distance [4, 93, 96]. Thus, when construals are psychologically proximate, they will exhibit low-level features; when they are psychologically distal, they will exhibit high-level features. Crucially, the delivery of a fear appeal that is proximate—rather than distant—should increase both the personal relevance of the threat and the consequent efficacy—yielding a more effective fear appeal.

Hypothesis development

Next, we propose hypotheses that explain why *message abstractness* (H1) and *context* (H2) may affect recipients' responses to fear appeals. Figure 1 illustrates our research model.

Message abstractness: The effect of concrete and abstract fear appeals

Again, the central tenet of CLT is that people judge objects, events, or actions in terms of either *feasibility* or *desirability* and, accordingly, form concrete or abstract construals to support this judgment [57, 92, 96]. CLT proposes that these concrete or abstract construals are thus either specific and psychologically proximate or generic and psychologically distal [4, 96]. Fear-appeal recipients may similarly form concrete and abstract construals to enable a specific type of judgment. If a recipient forms a concrete construal, the fear appeal will be evaluated in terms of the feasibility of the depicted threat event and action recommendation. In such circumstances, recipients will consider "*How* am I at risk?" and "*How* can I protect myself?" In contrast, if an abstract construal is formed, the fear appeal will be evaluated in terms of the desirability of the depicted threat event and

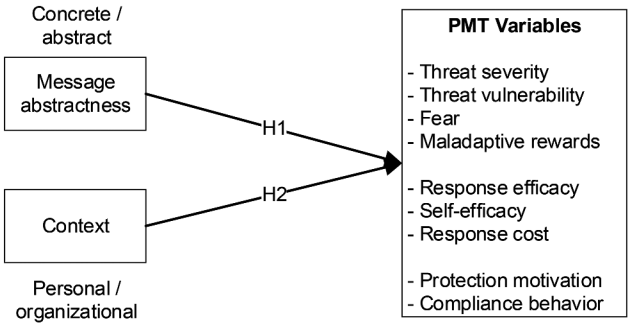

Figure 1. Research model.

action recommendation. Recipients will consider "*Why* do I need to avoid this threat?" and "*Why* should I perform this response?"

Fear appeals influence which construals are formed. This is because (1) *concrete fear appeals* can provide specific, low-level details that stimulate the formation of concrete construals, whereas *abstract fear appeals* can provide more generic details that stimulate abstract construals. Furthermore, (2) concrete fear appeals can suggest that a threat is proximate (i.e., imminent), thereby stimulating psychological proximity, which leads to the formation of concrete construals. In contrast, abstract fear appeals suggest a *general threat*, creating higher levels of psychological distance, which support the formation of abstract construals. Multiple studies have shown that construal level can be influenced by manipulations of message content (e.g., feasibility vs. desirability arguments, abstract descriptions vs. concrete pictures) [e.g., 18, 29, 31] and by manipulations of psychological distance [e.g., 16, 18, 42].

We uniquely posit that the recipient's construal level influences the efficacy of a fear appeal to stimulate appraisal perceptions. As laid out by PMT, fear-appeal appraisal is primarily concerned with perceptions of threat, efficacy, and response perceptions. Such perceptions are, however, informed by the recipient's underlying construal [96]. Thus, it is plausible that differences in construal level influence how a recipient judges and subsequently perceives threats and responses.

We thus specifically propose that PMT variables that are informed by judgments of *how* one is at risk (i.e., through the constructs of threat severity and threat vulnerability) and *how* one can cope with this risk (i.e., through the constructs of response efficacy and self-efficacy) will be informed by concrete construals. This is because such judgments serve the purpose of assessing feasibility (i.e., how an event or action will unfold). In contrast, PMT variables that are informed by judgments of *why* a risk is desirable (i.e., maladaptive rewards) or *why* a response is undesirable (i.e., response cost) will be informed by abstract construals. Thus, whether a message evokes concrete or abstract construals will affect its capacity to stimulate specific appraisal variables.

If this holds, concrete fear appeals will be more efficacious in raising threat perceptions. Research has shown that people focus more strongly on negative features when they are described concretely [23, 24] and that describing negative consequences in fear appeals increases threat severity perceptions [54]. Concrete construals have also recently been

linked to increases in vulnerability perceptions [14]. Given that concrete messages are also generally perceived to be more truthful [29], we propose:

Hypothesis 1a (H1a): ***Concrete fear appeals*** *increase recipients' perceptions of* ***threat severity***.

Hypothesis 1b (H1b): ***Concrete fear appeals*** *increase recipients' perceptions of* ***threat vulnerability***.

We further propose that concrete fear appeals will be more efficacious in raising response perceptions. Related research in marketing has already shown that concrete fear appeals can lead to increases in response efficacy and self-efficacy [31]. It may be that "seeing" the recommended behavior in a concrete message facilitates understanding and thus leads to higher response and self-efficacy perceptions [102]. Other research suggests that users' perceived need to perform an activity sooner (i.e., proximate psychological distance) may also lead to stronger self-efficacy beliefs [60]. Thus,

Hypothesis 1c (H1c): ***Concrete fear appeals*** *increase recipients' perceptions of* ***response efficacy***.

Hypothesis 1d (H1d): ***Concrete fear appeals*** *increase recipients' perceptions of* ***self-efficacy***.

In contrast, we expect that concrete fear appeals will be *less* efficacious in raising cost and reward perceptions. We thus propose:

Hypothesis 1e (H1e): ***Concrete fear appeals*** *foster lower levels of* ***maladaptive rewards*** *than* ***abstract fear appeals***.

Hypothesis 1f (H1f): ***Concrete fear appeals*** *foster lower levels of* ***response costs*** *than* ***abstract fear appeals***.

Based on later PMT research, it follows that increased threat severity and threat vulnerability perceptions lead to increased fear [9, 27, 82]. Thus, if concrete threat representations exert a positive effect on threat severity and threat vulnerability perceptions, fear should increase. Employees are more likely to experience fear when perceiving that a spear phishing attack is imminent (vs. in the future), targeted at themselves (vs. others), or may lead to devastating personal consequences (vs. vaguely defined consequences). From a CLT perspective, the resulting concrete construals are associated with fear responses [96]. Thus,

Hypothesis 1g (HQ1g): ***Concrete fear appeals*** *yield higher levels of* ***fear*** *than* abstract fear appeals.

Finally, we predict that concrete threat representations will more readily elicit protection motivation and compliance behavior. This logic follows from PMT's prediction that perceived threat severity, perceived threat vulnerability, and fear positively influence protection

motivation [9, 27, 82]. From a CLT perspective, this argument is consistent with findings that indicate that concrete (vs. abstract) threat depictions are superior motivators of avoidance goals. For example, a study by Semin et al. [84] found that abstract messages are less persuasive than concretely worded messages for protective purposes. In combination with evidence that concrete messages are generally perceived as more truthful [29], we expect concrete threat representations to be more persuasive. Finally, given that PMT conceptualizes protection motivation as a predictor of subsequent behavior [95], we hypothesize:

Hypothesis 1h (H1h): ***Concrete fear appeals*** *yield* *higher levels* *of* ***protection motivation*** *than* ***abstract fear appeals***.

Hypothesis 1i (H1i): ***Concrete fear appeals increase*** *actual* ***security compliance behavior***.

Difference between personal and organizational audiences

Next, we examine why the utility of PMT for explaining how fear appeals lead to behavioral change may be context dependent. Notably, "theories in the social sciences are not applicable irrespective of context" [13, p. 576]. *Context* is typically defined as the "situational opportunities and constraints" [13, p. 386] that surround the phenomenon under investigation [3]. Contextual factors may be powerful boundary conditions that regulate the applicability of theories [13] by, for example, affecting the relationships between variables [46]. Moreover, "no theory is always wrong or always right—all are more or less relevant and helpful in different situations" [1, p. 1272]. However, the situations to which this principle applies may be unknown, because theories developed primarily in a single context are often agnostic regarding contextual factors, which remain largely "unmeasured and unmentioned" [39, p. 112]. Consequently, PMT may suffer from similar contextual constraints because it originated outside of ISec research; constraints that are not yet fully clear may materialize when contextual boundaries are traversed [13].

Interestingly, there seem to be no such constraints when applying PMT to the ISec context with personal users. Multiple studies have found that PMT is useful for explaining individual responses to personal security threats [e.g., 9, 66]. This may be the case because personal security contexts are sufficiently similar to healthcare contexts in that the main factors that influence a recipient's behavior primarily concern the individual self. If this is true, then PMT can be highly effective in such contexts because all its constructs are related to self-perceptions. For example, PMT suggests that individuals' behavior is driven by perceptions of a threat to the self.

However, unspecified constraints may limit the utility of PMT when applied in ISec contexts with organizational users, which are rich in higher-level factors that may influence individual attitudes and behaviors [12]. We assert that PMT does not account for these factors, and that its power (utility) for explaining organizational users' responses to fear appeals may, therefore, be limited. Again, the appraisal factors of PMT relate predominantly to the threat (i.e., threat severity), the response (i.e., response efficacy), and their relationship to the self (i.e., threat vulnerability, self-efficacy, maladaptive rewards, response cost). However, additional organizational factors also influence how employees respond to fear appeals. For example, employees' training, experience with

phishing attacks, or their general attitude toward the organization may affect employees' response to fear appeals. For instance, a study by Posey et al. [77] showed that PMT predicts behavioral outcomes only among employees with strong affective organizational commitment and, thus, introduces an organization-related factor that moderates the key outcome of PMT. Other studies have shown that PMT can be extended by considering factors such as workplace policies [8, 50], workplace norms [34], and peer behaviors [2]. Finally, some researchers claim that because organizational threats lack personal relevance, fear appeals will not be as effective, especially in terms of generating fear [cf. 50, 101]. Thus,

Hypothesis 2 (H2): Responses of ***organizational users*** *to fear appeals will be lower than fear-appeal responses of personal users—manifesting in lower (a)* ***threat****, (b)* ***fear****, and (c)* ***protection motivation****.*

Study 1: Personal users

We test our theoretical model in the domain of spear phishing, because it is a pervasive threat that can be relevant to individuals as well as organizations. *Spear phishing* is a highly targeted, context-specific attack directed at specific groups of individuals or organizations that aims to appear authentic to message recipients [99]. Spear phishers attempt to exploit employees by sending emails that appear to be legitimate requests (via social engineering) to elicit personal data necessary to access organizational systems and data. Compared to other phishing techniques, spear phishing is considered more sophisticated [38] and exponentially more dangerous to individuals [44]. Thus, spear phishing is relevant to personal and organizational security.

Investigating the effect of fear appeals as a motivational strategy for mitigating spear phishing is particularly promising because although firms often offer anti-spear-phishing training, empirical evidence suggests that employees often fail to internalize their security education [56, 78, 88, 89]. Thus, typical antiphishing training often does not motivate employees, because it is often lengthy, disruptive, and onerous, thus making typical training less motivating for users than more engaging training techniques [5, 88]. As a result, even trained individuals with advanced security knowledge fall prey to phishing attacks, arguably because they are not motivated to apply the basic training principles necessary to detect cues that a message is illegitimate [45, 100, 108]. Thus, exploring how to craft concrete or abstract fear appeals to stimulate higher user motivation in complying with security training affords opportunities to contribute to an important problem.

Study 1 research design

To test H1, we began with an experiment conducted in a personal context. For this experiment, we developed concrete and abstract anti-spear-phishing fear appeals, deployed them, and measured participants' threat perceptions, fear, and protection motivation. Our treatments and measurements were reviewed by several ISec scholars and pilot tested before the full data collection.

Study 1 participants

Our targeted sample frame was personal users, referring to users that use computers for personal purposes. To that end, we recruited computer users from Amazon Mechanical Turk (MTurk) and solicited participation by offering a monetary incentive. Studies have shown that results based on data gathered from MTurk are comparable to those based on data acquired through other means [40, 65, 72, 91], but the key is taking careful steps to increase data quality [58, 91], which we followed. We restricted the MTurk participant pool to expert workers (workers with a record of providing quality data) who were employed and based in the United States. Participants also had to answer the survey using a computer, logically ensuring that we were recruiting computer users. We evaluated participants' attentiveness by employing multiple attention checks, monitoring the time they spent on the survey and manipulations, and asking questions to ensure that the manipulations were well received. Of the 112 responses collected, 28 were removed because participants did not finish within the same day or took less than four minutes to complete the entire instrument. The remaining 84 responses were sufficient to obtain a statistical power of 0.8 for the detection of medium effects (Cohen's $d \geq 0.5$) [25]. Participants spent an average of 15 minutes on the survey (Supplemental Online Appendix 3 provides the sample characteristics). The demographics were comparable between treatment groups, indicating successful random assignment of participants to groups.

Study 1 procedures

The experiment was carried out via the online survey software Qualtrics, and the steps were as follows: (1) Participants provided demographic information; (2) participants were randomly assigned to the two treatment conditions and were shown the treatment videos; and (3) participants were subsequently asked to answer a survey that captured their perceived concreteness/abstractness of the received treatment (manipulation check) and relevant psychometric constructs. Supplemental Online Appendix 2 provides operational details of the procedures. We used videos to deliver our manipulations because video is a familiar medium on the Internet and is a common and increasingly effective way of delivering training [43]. Thus, in contrast to text manipulations, the use of videos allowed us to increase the *ecological validity* of our experiment, which is an especially important consideration in ISec research [59].

Study 1 manipulations

We constructed our abstract fear appeals by manipulating threat representation in two ways. First, because abstract construals describe events with high-level features, we described the threat of spear phishing using high-level terms that focus on desirability (e.g., why spear phishing is dangerous) with high-level features (e.g., can severely affect finances and reputation). These manipulations are in line with studies in the reference literature that use desirability framing (e.g., "why") [29, 35] and abstract language [55]. Second, because abstract construals are associated with high levels of psychological distance, we included terminology that indicated high psychological distance (e.g., "it's a threat that may hypothetically affect users around the world in the future").[4] We leveraged the relevant terms for low and high psychological distance from [4].

Likewise, we constructed our concrete fear appeals by manipulating our description of spear phishing in two ways. First, we focused on the feasibility aspects by describing the

threat in detail (e.g., how spear phishing works) and detailing low-level features (e.g., "a criminal can take out loans under your name"). Second, we included language that suggested low psychological distance (e.g., "it is a threat that may realistically affect you here in the present"). The manipulations were pilot tested with MTurk participants and deemed effective.

Our manipulations were delivered via animated videos that integrated text, images, and voice-over speech. For each treatment, the fear appeal was delivered in two parts: The first provided the threat manipulation, and the second detailed the coping recommendation.[5] The lengths of the videos varied, because concrete threat representations require the delivery of more detail than abstract threat representations. This is congruent with CLT, which defines abstract construals as more "impoverished" than concrete construals [96]. We discuss potential confounds in the Limitations section, but felt this choice was preferable over inflating the abstract treatment with unnecessary content that could have impeded participants' attention to our manipulation. Another study by Köhler [55] chose a similar approach for creating concrete messages by adding more detail, thus creating longer manipulations.

To ensure that only abstractness and psychological distance differed between the treatments, we provided the same information on different abstract levels in both treatments (e.g., "financial loss" in the abstract treatment was presented as "someone buying goods with your credit card" in the concrete treatment). Supplemental Online Appendix 2 presents the scripts and links to the relevant videos. The treatments were previously pretested in a pilot and deemed successful, but minor changes were made to improve clarity.

Moreover, to assess the effectiveness of our abstractness and psychological distance manipulations, we drew guidance on manipulation checks from [4, 35]. We thus asked questions about whether the treatment was focused on the attributes and anatomy of the threat (i.e., concrete) or the general desirability of the threat itself (i.e., abstract) [cf. 35]. Furthermore, we assessed participants' psychological distance to the threat using bipolar scales with related linguistics [4]. Our treatments were successful: We engendered *very large* and *large* effects on perceived threat abstractness ($\Delta M = 1.95$, $p = 0.00$, Cohen's $d = 1.21$) and threat psychological distance ($\Delta M = 2.13$, $p = 0.00$, Cohen's $d = 1.19$).

Study 1 measurement and controls

We measured the PMT constructs of threat severity, vulnerability, maladaptive rewards, response efficacy, self-efficacy, response costs, and protection motivation based on the instrument developed in [47, 50]. We measured fear responses based on [9]. The final behavior was observed (recorded) when participants chose to learn more about phishing. We also included a marker variable to test and correct for monomethod bias ex post facto [76]. Control variables were based on previous literature on phishing and fear appeals and included gender, education, age, computer use, computer self-efficacy in ISec, Web experience, ISec knowledge, suspicion, prior antiphishing training, exposure to media, and prior phishing victimization (self and others) [9, 63, 79, 109]. Supplemental Online Appendix 2 provides the full details of the measurement instruments.

Table 3. Study 1 MANCOVA results.

	Treatment		MANCOVA Results[6]	
Dependent Variables	Abstract Mean (SD)	Concrete Mean (SD)	*p*-value	Partial η^2
Threat severity (H1a)	5.87 (0.88)	6.40 (0.68)	**0.00**	**0.10**
Threat vulnerability (H1b)	4.30 (1.58)	5.18 (1.27)	**0.01**	**0.09**
Response efficacy (H1c)	6.35 (0.58)	6.41 (0.69)	0.66	0.00
Self-efficacy (H1d)	5.70 (0.73)	5.56 (1.03)	0.45	0.01
Maladaptive rewards (H1e)	2.78 (1.50)	2.71 (1.72)	0.85	0.00
Response costs (H1f)	1.90 (0.87)	1.61 (0.82)	0.12	0.03
Fear (H1g)	3.19 (1.38)	3.92 (1.37)	**0.02**	**0.07**
Protection motivation (H1h)	4.39 (1.79)	5.21 (1.60)	**0.03**	**0.06**

Notes: MANCOVA, multivariate analysis of covariance.

Across the sample, all measured constructs in the model and the manipulation check passed reliability (Cronbach's $\alpha \geq 0.7$) [61] and validity checks (convergent validity: AVE > 0.5, discriminant validity: square root of AVE > interconstruct correlations) [61]. Multicollinearity was not an issue, as variance inflation factors were below 3.00 [30] and item communalities were above 0.80. Based on the widely used correlation-based marker variable approach with a theoretically unrelated variable [104], we ascertained that our findings are robust to common method bias. See details in Supplemental Online Appendix 3.

Study 1 results

H1 hypothesized that concrete fear appeals would increase fear-appeal outcomes. To test H1, we analyzed our data using a multivariate analysis of covariance (MANCOVA) via IBM SPSS v24. We ran the message as a fixed factor and included controls as covariates, as shown in Table 3. Our results indicate that concrete fear appeals lead to increases in perceived threat severity ($p = 0.00$), perceived threat vulnerability ($p = 0.01$), fear ($p = 0.02$), and protection motivation ($p = 0.03$) (H1a, H1b, H1g, and H1h are supported). Importantly, these effects are of *medium* effect size. Our analysis shows no significant effects of concrete fear appeals on maladaptive rewards, response efficacy, self-efficacy, and response costs; thus, H1c–f are not supported. This suggests that concrete fear appeals are more effective than abstract fear appeals in stimulating threat perceptions, engendering fear, and raising protection motivation. It is thus possible that message abstractness has no influence on raising efficacy perceptions.

Study 2: Organizational users

Study 2 research design

To test whether these effects could be replicated among organizational users (H1) and whether that organizational user context would itself have effects on fear-appeal appraisal (H2), we replicated Study 1 using full-time employees at a large US university. Universities often suffer from phishing attacks [110] and are thus a useful organizational context for studying fear appeals. Prior to our study, the sampled university had significant issues with

phishing attacks and consequently initiated extensive efforts to train staff and faculty. An executive at the cybersecurity operations center (CSOC) emphasized:

> *phishing remains a persistent problem for the university with technical solutions only preventing so many attacks. We continue to invest in training, warnings, and consulting to better defend attacks that bypass technical solutions and help individuals understand this problem at the university.*

Moreover, the CSOC provided statistics showing that in 2019 there were 337,640 attempted attacks. Of those attacks, 76.7%, or 286,582, were blocked by technical solutions. The remaining 51,058 bypassed technical countermeasures; of those, 246, or less than 1%, were responsible for university expenditures of approximately $490,000 (annually) devoted to addressing this problem. The CSOC directly traced the handful of attacks that had direct adverse financial effects on the university, which were caused by attacks that were able to compromise and change bank routing information. In response to these attacks, the university increased training frequency from annually to quarterly, disseminated mass campaign warnings monthly or as needed, and implemented training on the importance of compliance in protecting information during employee onboarding procedures.

Study 2 participants

The sampling frame of Study 2 was organizational computer users. In partnership with the university's chief information security officer and staff, we invited approximately 2000 staff and faculty (not students) from a large US university to participate in the study. An a priori power analysis suggested that this sample size is sufficient to detect medium effects (f = 0.25) with 80% confidence. Participation was solicited via emails sent out by the university's IT security function and were presented as part of the regular training program employed by our research site, which thus increased the probability that participants would perceive the solicitation email to be an authentic organizational communication. The participants were randomly assigned to the treatment conditions. Of the 222 responses obtained, we removed responses that did not complete the survey on the same day, resulting in 179 usable data points. The average time spent on the survey was 28 minutes; the fastest response took around 10 minutes. An explanation for the longer survey duration of Study 2, as compared to Study 1, is that the MTurk participants in Study 1 had more experience taking surveys than the participants in Study 2. The demographics across the treatment conditions are comparable (see Supplemental Online Appendix Table 3.5 for demographics); thus, we conclude that randomization was successful.

Study 2 manipulations

We used the same fear-appeal manipulations and manipulation checks that were used in Study 1. Consistent with Study 1, our fear-appeal abstractness manipulation yielded significant and large to very large effect sizes on the users' perceptions of threat abstractness (ΔM = 1.84, p = 0.00, Cohen's d = 1.41) and threat psychological distance (ΔM = 1.83, p = 0.00, Cohen's d = 1.02).

Study 2 procedures, measurement, and controls

The remaining procedures mirrored Study 1: The participants first provided their demographic information and were randomly assigned to abstract or concrete fear-appeal conditions. Next, they received the fear-appeal treatment, and then answered the manipulation check questions and responded to the PMT instruments. The overall measurement was identical to that of Study 1. All construct measures for the PMT and manipulations were over the 0.7 threshold for Cronbach's α, except the threat feature (0.69). As in Study 1, all measured constructs exhibited convergent validity (i.e., AVE > 0.5) and discriminant validity (i.e., square root of AVE > interconstruct correlations) [61]. Multicollinearity was not an issue, as all construct variance inflation factors were again below 3.00 [30]. All item communalities were above 0.80, and all correlations were within a reasonable range. Using the correlation-based marker variable approach, we ensured that all findings were robust to common method bias. Supplemental Online Appendix Table 3.7 provides the measurement model statistics.

Study 2 Results

To determine whether concrete fear appeals also improve fear-appeal outcomes (H1) in organizational contexts, we analyzed the data through a MANCOVA conducted in IBM SPSS v24. Table 4 reports the results. Our results indicate that H1a, which posits that concrete fear appeals improve threat severity perceptions, is supported in organizational contexts ($\Delta M = 0.26$, $p = 0.05$, $\eta^2 = 0.02$). We also found support for our claim that concrete threat representations stimulate higher protection motivation (H1h) in organizational contexts ($\Delta M = 0.39$, $p = 0.04$, $\eta^2 = 0.02$). Additionally, we found a significant negative effect for (H1f), which posited the effect of concrete fear appeals on participants' perceived response costs ($\Delta M = -0.30$, $p = 0.04$, $\eta^2 = 0.02$). However, our results reveal no significant effect of concrete messages on threat vulnerability (H1b) and fear (H1g) for organizational users, indicating that user context may affect how people appraise ISec threats and efficacy.

Personal vs. Organizational users

To further investigate the role of user context in recipients' threat appraisals, we compared the Study 1 and 2 data, which used identical manipulations and survey

Table 4. Study 2 MANCOVA results.

	Treatment		MANCOVA Results[7]	
Dependent Variables	Abstract Mean (SD)	Concrete Mean (SD)	*p*-value	Partial η^2
Threat severity (H1a)	6.11 (0.8)	6.37 (0.79)	**0.03**	**0.03**
Threat vulnerability (H1b)	4.53 (1.43)	4.51 (1.62)	0.90	0.00
Response efficacy (H1c)	6.27 (0.67)	6.27 (0.65)	0.99	0.00
Self-efficacy (H1d)	5.15 (0.95)	5.22 (1.18)	0.63	0.00
Maladaptive rewards (H1e)	2.72 (1.47)	2.34 (1.36)	0.07	0.02
Response costs (H1f)	2.21 (0.98)	1.91 (0.96)	**0.04**	**0.02**
Fear (H1g)	3.94 (1.24)	3.91 (1.27)	0.85	0.00
Protection motivation (H1h)	5.30 (1.32)	5.70 (1.21)	**0.04**	**0.02**

Notes: MANACOVA, multivariate analysis of covariance.

Table 5. MANCOVA results Study 1 vs. Study 2.

	Concrete			Org. User			Concrete x Org. User		
Construct	ΔM	*p*-value	*p*. η^2	ΔM	*p*-value	*p*. η^2	ΔM	*p*-value	*p*. η^2
Threat severity (H1a)	**0.35**	**0.00**	**0.05**	0.13	0.30	0.00	0.50	0.19	0.01
Response efficacy (H1b)	0.02	0.72	0.00	-0.11	0.21	0.01	-0.08	0.72	0.00
Threat vulnerability (H1c)	**0.26**	**0.03**	**0.02**	-0.19	0.27	0.00	**0.21**	**0.02**	**0.02**
Self-efficacy (H1d)	-0.01	0.79	0.00	**-0.45**	**0.00**	**0.04**	-0.48	0.40	0.00
Maladaptive rewards (H1e)	-0.29	0.25	0.01	-0.21	0.28	0.00	-0.44	0.42	0.00
Response costs (H1f)	**-0.29**	**0.02**	**0.02**	**0.30**	**0.01**	**0.02**	0.02	0.97	0.00
Fear (H1g)	**0.22**	**0.04**	**0.02**	**0.40**	**0.03**	**0.02**	**0.72**	**0.02**	**0.02**
Protection motivation (H1h)	**0.55**	**0.00**	**0.04**	**0.73**	**0.00**	**0.05**	1.30	0.27	0.00

Notes: MANACOVA, multivariate analysis of covariance. *P*. η^2 = partial η^2; $\eta^2 \geq 0.06$ is considered a medium effect size and $\eta^2 \geq 0.14$ a large effect size.

instruments. The identical research design established configural and compositional measurement invariance, which enabled analysis of the differences between the data sets through the introduction of an additional grouping factor [33]. We therefore introduced the data source as a dummy treatment factor (personal vs. organizational users) and analyzed the data using a MANCOVA via IBM SPSS v24. Including demographic variables in the model would have led to endogeneity because the assumption of independence between independent variables would have been violated. Table 5 summarizes these results.

When controlling for the influence of context, we found that concrete fear appeals lead to significant increases in threat severity (H1a), threat vulnerability (H1c), fear (H1f), and protection motivation (H1g). Beyond that, we found evidence supporting H1f, which hypothesized that concrete threat representations decrease response costs perceptions (ΔM = -0.29, p = 0.02, η^2 = 0.02). This suggests that concrete fear appeals make for stronger and more effective interventions than abstract fear appeals.

Sampling from organizational users instead of personal users affected fear-appeal appraisal variables. We predicted that our fear appeal would evoke lower threat severity and threat vulnerability (H2a), fear (H2b), and protection motivation (H2c) among organizational users. When controlling for differences in message abstractness, we found that the fear-appeal application led participants to report higher fear perceptions (ΔM = 0.40, p = 0.03, η^2= 0.02) and protection motivations (ΔM = 0.73, p = 0.00, η^2= 0.05), thus supporting H2c and H2d. This implies that organizational users report higher levels of fear, response costs, and protection motivation than personal users. However, this pattern did not hold for threat severity (H2a) and threat vulnerability (H2a). For the response portion of PMT, we found that the organizational contexts yielded significant effects on self-efficacy (ΔM = -0.45, p = 0.00, η^2= 0.04) and response cost (ΔM = 0.30, p = 0.01, η^2= 0.02), which suggests that organizational users perceive lower self-efficacy and response costs than personal users.

Considering the interaction between the two factors, we found significant effects on threat vulnerability (ΔM = 0.21, p = 0.02, η^2= 0.02) and fear (ΔM = 0.72, p = 0.02, η^2= 0.02), implying that the ability of concrete fear appeals to increase threat vulnerability perceptions and fear is moderated by context. This finding may thus explain why the associated hypotheses H1c and H1g were significant in Study 1 but not in Study 2.

Study 3: Robustness check of construal-level manipulation

Although Studies 1 and 2 provide support for our hypothesis that message design influences the efficacy of fear appeals, these studies have three limitations. First, the video-based treatments differ in length, which may be a confounding factor leading to biased results. Second, since these studies did not use behavior as an outcome variable, thus it cannot be ascertained whether message design increases the likelihood that individuals will comply with what is advocated in the fear appeal. Third, although Studies 1 and 2 provided support for our hypotheses, these studies did not explicitly test whether their results were caused by the theorized mechanism of concrete and abstract fear appeals influencing construal level.

To address these limitations, we performed a conceptual replication of the experiments in the context of home network threats. Home network threats target the computer networks of users' homes (i.e., WiFi routers) and thus threaten users' personal IT assets that are connected to such networks. This replication required further modifications to the research design of Studies 1 and 2 because it used text-based treatments of equivalent length, measured dichotomous behavioral outcomes, and included further checks to assess the influence of our treatments on construal level. Notably, although our modifications do not present a threat to the validity of the replication, if our findings can be reconfirmed using a modified methodology and a slightly different threat context, this would further bolster the support for our hypotheses [70].

Study 3 research design

Study 3 participants and procedures

As in Study 1, we recruited from Mturk and offered a substantial monetary incentive. This experiment was also conducted via Qualtrics. Again, following established guidelines, we restricted the participant pool to US citizens that had been verified as expert workers with a track record for good data and we also employed attention traps [58, 91]. Given recent claims that foreign workers use VPNs to access the U.S. survey pool and may even provide multiple responses,[8] we employed several additional sophisticated measures to ensure high-quality data. These measures included checks for participants' attention that requested answers to reverse-coded questions (e.g., comparing participants' answers for "I'm organized" vs. "I'm disorganized"), English-proficiency screening questions (using grammar and vocabulary), evaluations of time spent on the treatment, and open feedback analysis. After applying these quality assurance measures, we were left with a total of 264 valid responses out of the 300 that we originally solicited. Supplemental Online Appendix 3 details the demographics. The sample comprised slightly more males than females (55%); the average participant was 37.4 years of age and had a bachelor's degree, 21.9 years of computer experience, and 19.2 years of Internet experience. Between our treatment groups, we found no significant differences regarding these sample characteristics, indicating that randomization was successful.

We employed the following experimental procedures: Participants were recruited via Mturk and randomly assigned to one of two experimental conditions. Next, participants received the fear-appeal manipulation and were subsequently presented with an option to perform or decline to perform the recommended behavior. Then, participants were asked

to answer a survey that captured their perceived concreteness/abstractness of the received treatment (manipulation check) and relevant psychometric constructs before providing demographic information.

We also chose to measure behavior immediately after the treatment and prior to any other psychometric measures. We took this approach for two reasons. First, it helped minimize the potential for treatment effects to dissipate before the outcome of interest could be measured. Second, it helped preempt the threat that participants' responses to questionnaire items would bias their behaviors.[9] This design increased our confidence that any potential findings regarding behavioral change could be legitimately attributed to the treatment effects.

Study 3 manipulations

To address the video format as a potential threat to validity, we developed concrete and abstract manipulations using text messages of similar length. Again, to develop concrete messages, we constructed arguments that emphasized feasibility, whereas abstract messages were developed using arguments that emphasized desirability. This operationalization closely follows existing research on CLT and persuasion [28, 31, 32]. In line with PMT, we formulated "how vs. why" arguments pertaining to each PMT variable—threat severity, threat vulnerability, maladaptive rewards, response efficacy, self-efficacy, and response cost [9]. The messages were of similar length and provided the same number of arguments.

Notably, we did not manipulate psychological distance but focused solely on providing concrete and abstract messages. If our theorizing is correct, we expect that (1) concrete or abstract messages will be sufficient to stimulate changes in construal level and elicit the hypothesized effects, and (2) treatments that do not manipulate psychological distance will have lower effects compared to treatments that manipulate both congruently (as did Studies 1 and 2). We added a manipulation check to determine whether our treatments yielded effects on the construal level. Supplemental Online Appendix 2 presents the treatments and manipulation check measures. The manipulations led to significant differences in participants' perceptions of message abstractness ($p \leq 0.00$) and construal abstractness ($p = 0.01$). The effects of these manipulations were medium and small, whereas the effects of the manipulation in Studies 1 and 2 were large (Supplemental Online Appendix 3). The differences in effect sizes are may be due to the omission of the additional manipulation of psychological distance, which, if true, would have implications for how researchers should operationalize fear appeals.

Study 3 measurement and controls

Another purpose of this replication was to measure objective behavioral change. Prior fear-appeal studies in the ISec context have never attempted to *observe* the effects of fear appeals; the few studies that have measured behavior have used post hoc self-reported measures [e.g., 9, 77]. In the absence of published research designs in the ISec literature to guide our inquiry, we drew on research designs from the original healthcare literature, which typically assess dichotomous behavioral outcomes (i.e., whether or not a recipient complied with a fear appeal) [68].

In doing so, it is important to note that the purpose of a fear appeal is primarily motivational to encourage performance of a specific behavior [80, 81]. Consequently, fear

appeals are commonly used to encourage recipients to perform simple behaviors, such as "apply sunscreen" or "get a preventive skin cancer examination" [95], but typically do not include detailed instructions on how to perform these behaviors, aside from encouraging general efficacy. Similarly, ISec fear appeals typically recommend behaviors that recipients can develop the efficacy to perform, assuming they are motivated to do so through threat. Examples are ISec fear appeals that encourage people to "always log off your computer" or "perform a password change" [50]. Thus, if fear appeals are to be evaluated in terms of behavioral outcomes, these outcomes must be clear and unequivocal so that participants' motivation can be isolated as the primary determinant of behavior performance.

Accordingly, we observed whether participants followed a link for vulnerability scanner software. We maintain that it can be assumed that each participant could follow a link to a landing page, especially because we recruited participants via a Web portal. This behavior thus meets the aforementioned criteria for what behavioral changes can pragmatically be measured based on fear-appeal treatments. Moreover, a participant following a link is a meaningful behavioral outcome, as corroborated by the practice of using clicks to measure the effectiveness of advertisements. Google charges its advertisers $1-2 per ad click [85], and we can assume that advertisers would be unwilling to pay for such clicks if they did not meaningfully convert into sales. Thus, we apply the same logic here and surmise that it is a particularly meaningful outcome to show a participant chose to visit the intended website.

To measure the psychometric PMT constructs, we used the same tested instrument used in Studies 1 and 2. However, Study 3 required some item-level adaptation because we changed the context of the study from spear phishing to home network threats. Furthermore, because the participants in Study 3 performed the behavior prior to the measurement of protection motivation, we changed the wording of that measurement to reflect the intentions present when the behavior was changed. Study 3 measured the same covariates and demographics as Studies 1 and 2. The measurement instrument validity statistics indicated high reliability and validity; specifically, the measurement statistics for all constructs yielded a Cronbach's α above the 0.7 threshold and AVE scores above the 0.5 threshold [61]. Furthermore, our measurements indicated discriminant validity in that the square root of AVE for each construct was smaller than all possible interconstruct correlations [61]. Multicollinearity was unproblematic: variance inflation factors were again below 3.00 [30] and item communalities were again above 0.80. Further measurement details are provided in Supplemental Online Appendix 3.

Study 3 data analysis and results

Study 3 MANCOVA

We began our analysis by testing the effect of message abstractness on PMT variables (Table 6). Again, we performed a MANCOVA using IBM SPSS v24 and found that concrete messages lead to significant effects on threat vulnerability ($p = 0.02$), response cost ($p \leq 0.05$), fear ($p = 0.00$), and protection motivation ($p = 0.03$). These findings support H1c, H1f, H1g, and H1h, respectively.

Table 6. Study 3 MANCOVA results.

	Treatment			
	Abstract	Concrete	MANCOVA Results[10]	
Dependent Variables	Mean (SD)	Mean (SD)	*p*-value	Partial η^2
Threat severity (H1a)	5.46 (1.06)	5.74 (0.98)	0.11	0.01
Threat vulnerability (H1b)	4.31 (1.16)	4.63 (1.08)	**0.02**	**0.02**
Response efficacy (H1c)	5.44 (1.02)	5.66 (0.95)	0.38	0.00
Self-efficacy (H1d)	4.86 (1.01)	5.10 (1.07)	0.21	0.01
Maladaptive rewards (H1e)	3.56 (1.24)	3.38 (1.13)	0.32	0.00
Response costs (H1f)	3.06 (1.22)	2.64 (1.17)	**0.05**	**0.02**
Fear (H1g)	4.50 (1.3)	4.96 (1.28)	**0.00**	**0.03**
Protection motivation (H1h)	3.54 (1.7)	4.10 (1.64)	**0.03**	**0.02**

Notes: MANCOVA, multivariate analysis of covariance.

Study 3 binary regression

Next, we explored whether our manipulations influenced participants' behavior. We observed participants' behavior as a binary outcome (i.e., whether they followed the fear appeal's recommendation). Our descriptive statistics suggest that, across treatment conditions, substantially more participants (145 out of 264, or 55%) chose to perform the recommended behavior (Table 7). Furthermore, the descriptive statistics suggest that more participants in the concrete condition (61%) were willing to comply with the fear appeal than in the abstract condition (41%).

To test whether concrete messages lead to different behavioral outcomes, which we observed as a dichotomous variable in our research design, we estimated and evaluated a binary logistic regression model (Table 8), following established guidelines [73]. In the estimation, we could not include PMT variables, because they are influenced by the message treatment and are therefore not independent—a core assumption of regression models. Thus, we included message abstractness as a factor and our control variables as covariates. The estimated model yielded a χ^2 (11) of 41.73 ($p \leq 0.00$), indicating that the model describes the data better than an intercept-only model. The Wald's χ^2 scores also

Table 7. Description of response variable.

Complied with Fear Appeal?	Abstract	Concrete	Total
No (coded as 1)	84	35	119
Yes (coded as 2)	58	87	145
Summary	142	122	264

Table 8. Binary logistic regression.

Predictor	β	Wald's χ^2	df	*p*	Exp (B)
Constant	0.02	0.00	1	0.99	1.02
Message abstractness	-1.31	21.80	1	0.00	0.27
Gender	-0.09	0.09	1	0.77	0.92
Age	0.00	0.00	1	0.99	1.00
Education	-0.24	3.28	1	0.07	0.79
Job in IT?	0.01	0.16	1	0.69	1.01
Computer experience	-0.02	0.26	1	0.61	0.98
Internet experience	0.08	3.03	1	0.08	1.09
Web experience	0.04	1.50	1	0.22	1.04
Suspicion	-0.11	0.93	1	0.34	0.90
Risk	0.20	0.49	1	0.49	1.22
ISec computer self-efficacy	0.00	0.00	1	0.98	1.00

indicate that only message abstractness ($p \leq 0.00$) significantly predicted the dichotomous behavioral outcome. Two other predictors—namely, education and Internet experience—came close but did not surpass the 0.05 confidence threshold. We assessed goodness-of-fit through the Hosmer-Lemeshow (H-L) test [41] and Nagelkerke's pseudo R^2. The H-L test yielded a χ^2 (8) of 4.82 and was insignificant ($p = 0.78$), indicating that the model fits the data well, as there were no significant differences between the observed and predicted outcomes [73]. Nagelkerke's R^2 yielded 0.20, suggesting that the model explains 20% of the variance in participants' behavior. Overall, this suggests that the model is useful for explaining participants' behavior. Specifically, we found that message abstractness yields a negative effect ($\beta = -1.31$, $p \leq 0.00$) on the likelihood of participants to comply with the fear appeal. The probability indicated that individuals in the concrete condition had a 78.8% probability of following the link to download the vulnerability scanner. We also found a discrete increase of 27.4% in the probability of following the link when including this condition (average marginal effect of the treatment). Collectively, these results support H1i, which proposes that concrete fear appeals increase compliance behaviors.[11]

Discussion

Fear appeals, which combine a message of threat and efficacy, are increasingly being used for personal and organizational security in both research and practice. Unfortunately, the results in various ISec contexts have been mixed and even contradictory, and a debate has emerged on whether the use of fear is appropriate in personal or organizational security contexts. Our research addresses these issues and proposes that differences in the degree of message abstractness (i.e., abstract vs. concrete) and context (i.e., personal vs. organizational) can explain and resolve these controversies. To test our theorization, we conducted a series of three experiments, which support most of our hypotheses. We conclude this manuscript by summarizing these results and exploring their implications for research, theory, and practice.

Summary of results

We began by testing the effects of degree of message abstractness (i.e., abstract versus concrete) on fear-appeal effectiveness. We found considerable evidence for the efficacy of *concrete fear-appeal messages* across all three experiments (see Table 9). In Study 1 (conducted in a personal context), we found evidence that concrete messages improve a fear appeal's efficacy to stimulate threat severity (H1a), threat vulnerability (H1b), fear (H1g), and protection motivation (H1h). In Study 2 (a replication of Study 1 conducted in an organizational context), we found evidence that confirmed these effects on threat severity (H1a) and protection motivation (H1h) and also found new evidence of an effect on response cost (H1f). In Study 3, (a conceptual replication with personal users that was designed to further probe the fear-appeal effects on behavioral change), we found further evidence that confirmed the effects on threat vulnerability (H1c), response cost (H1f), fear (H1g), and protection motivation (H1h). We also found that concrete fear appeals more effectively stimulate actual behavior than do abstract fear appeals (H1i).

We conclude that the degree of fear-appeal message abstractness has a consistent influence on both intentions and behaviors and concrete fear-appeal messages are more

Table 9. Overview of results of message abstractness.

Hypotheses	Study 1: Personal	Study 2: Organizational	Study 3: Replication
H1a: Concrete FA → Threat severity (+)	*Supported*	*Supported*	Not supported
H1b: Concrete FA → Threat vulnerability (+)	*Supported*	Not supported	*Supported*
H1c: Concrete FA → Response efficacy (+)	Not supported	Not supported	Not supported
H1d: Concrete FA → Self-efficacy (+)	Not supported	Not supported	Not supported
H1e: Concrete FA → Maladaptive rewards (-)	Not supported	Not supported	Not supported
H1f: Concrete FA → Response costs (-)	Not supported	*Supported*	*Supported*
H1g: Concrete FA → Fear (+)	*Supported*	Not supported	*Supported*
H1h: Concrete FA → Protection motivation (+)	*Supported*	*Supported*	*Supported*
H1i: Concrete FA → Compliance behavior (+)	*n/a*	*n/a*	*Supported*

Notes: Supported = The evidence suggests a statistically significant effect ($p < 0.05$); Not supported = The collected suggests that the effect is insignificant. [1] Note: Mixed findings can be due to a lack of statistical power. Thus, when the data is pooled, statistical power increases and effects can become significant.

effective than abstract messages. These differences alone can readily explain many of the conflicting literature findings. The findings of Study 1 and Study 2 that were confirmed by Study 3 provide especially compelling evidence for the generalizability of the related hypotheses, because replication with modified research designs is a sign of robustness [70]. The only hypotheses that could not be corroborated in any of our experiments were related to effects on response efficacy (H1c), self-efficacy (H1d), and maladaptive rewards (H1e).

Next, we tested whether context (i.e., personal versus organizational settings) influenced the efficacy of our fear appeals by comparing the results obtained in Study 1 (personal users) and Study 2 (organizational users). This was possible because Study 2 was a methodologically identical replication of Study 1. Our findings showed that participants from Study 2 responded with *higher* fear and protection motivation than participants from Study 1. Crucially, participants from Study 2 were organizational employees, whereas participants from Study 1 were personal users. Thus, this finding contradicts the hypothesis (H2) that fear appeals may *fail* to elicit fear and protection motivation among organizational users—an argument that motivated this study, as this is a common claim in the literature that has not been properly tested. Importantly, this finding is not a theoretical contradiction: the theoretical crux of an effective fear appeal is that it must be personally relevant to stimulate fear; correspondingly, we show that concrete fear appeals help stimulate fear and the desired protective response. Moreover, we found that organizational users voiced lower self-efficacy perceptions but higher response cost perceptions. Both findings are congruent with the broader fear-appeals literature, as they indicate that people struggle more significantly with ISec at work than in their personal lives—another reason that concrete versus abstract appeals are important. Moreover, we found an interaction effect between message abstractness and the sampling population. Specifically, we found that concrete messages help improve threat vulnerability perceptions and subsequent fear among organizational users.

Implications for research and practice

Our research makes several original contributions to ISec research. Although many studies have asserted that there is a need for strong fear-appeal manipulations [e.g., 9, 95, 107], our work uniquely reveals what constitutes a strong ISec manipulation. Namely, we show

that the degree of message abstractness consistently influences outcomes in a predictable way, such that concrete fear-appeal messages are more effective in stimulating appraisal variables and fostering behavioral change than abstract ones. Notably, the effects of message abstractness have not been considered in extant ISec fear-appeals research [e.g., 9, 50, 64, 66, 98, 101]. This finding thus substantially extends research and practice understanding of *how* fear appeals exert their effects on behaviors, because we show that message designers not only need to be concerned with *what* information is presented in fear appeals (which is explained by PMT) but also about *how* the information is presented in terms of degree of abstractness. Importantly, the effect sizes we observed were generally of a medium magnitude (see Study 1, Study 2, and Study 3 MANCOVA results), which means that not only is degree of abstractness a statistical significant consideration, it has substantial and meaningful influence on perceptual constructs and actual security behaviors (i.e., concreate fear appeals greatly increase actual security behaviors). This provides compelling evidence that message design for concreteness could be highly efficacious in changing actual security behaviors in practice.

Understanding the effect of fear appeal message's abstractness is of further scientific and practical utility [19], because it (1) informs the debate on the conflicting findings currently riddling the ISec literature and (2) may transform the way practitioners and researchers operationalize fear appeals. First, the notion of message abstractness provides a new perspective on why the ISec fear-appeals literature has produced mixed findings. For example, one argument has been that fear appeals lack personal relevance among organizational users and will thus be ineffective in raising threat perceptions and fear [50, 66, 101]. To support this argument, Warkentin et al. [101] conducted an fMRI experiment and provided results that they used to argue that fear appeals may fail to elicit fear responses in organizational contexts. However, this argument is tenuous because their evidence was gathered using highly invasive and unnatural fMRI responses with MBA students in a nonorganizational setting—a setting which could readily be dismissed as ecologically invalid [59] and not personally relevant, and thus not appropriate for studying the relevance of threat and fear in any fear-appeals approach [i.e., 27, 62, 82, 106, 107]. More problematically, given our original theorization, it also turns out that Warkentin et al. [101] used highly abstract fear appeals to make fear claims. In juxtaposition to their claims and evidence, in three experiments, we find corroborating evidence that abstract fear appeals—again, as used in the Warkentin et al. [101] study—are less effective in eliciting fear. Moreover, our findings show an interesting interaction effect in that the effect of message abstractness may even be enhanced among organizational users. Thus, our findings suggest that mixed findings should not be attributed to differences in context alone but to a combination of message and contextual factors.

Importantly, whereas prior research has often blamed "context" for differences but never articulated how context affects PMT appraisal variables [48, 50, 101], this study is the first to shed light on *what* appraisal factors are affected and *how*. Our findings show significant differences in how participants respond to fear appeals. This is a unique contribution of our research, which is the first to compare results based on data collected from identical fear-appeal applications among personal and organizational users. Specifically, our findings suggest that organizational users respond with lower perceptions of self-efficacy than personal users but higher perceptions of response costs, fear, and protection motivation. Thus, our research provides evidence of differences in how fear

appeals are appraised. Our findings show that there are indeed contextual differences when using fear appeals, especially in comparing personal and organizational contexts. As we have asserted, some of these differences can likely be attributed to organization-level factors that are currently not included in PMT. Our findings indicate that participants perceived lower perceptions of self-efficacy and higher response costs, both which negatively influence the persuasiveness of fear appeals. Thus, addressing these two factors may be particularly helpful in improving fear appeals that target organizational users.

Moreover, understanding how to integrate concrete threat and efficacy representations to create effective fear appeals is of scientific and practical importance because this influences how fear is generated and influences subsequent behavioral responses. This is especially fundamental, given that many extant ISec studies have unwittingly relied on abstract fear appeals. Furthermore, guidance on how to create strong fear appeals through concrete message design is missing. To provide needed guidance, we offer three design principles, rooted in CLT, and our empirical evidence for how to create effective fear appeals by representing threats concretely (Table 10). To develop strong fear appeals, we recommend crafting concrete messages with a focus on feasibility that explain—or literally show—the target audience how they are at risk (for instance, by giving concrete examples that illustrate an otherwise abstract threat). Then, in line with showing how a threat works, we recommend describing how the threat leads to negative consequences. Finally, we recommend specifying threats as being psychologically close by using language that is associated with psychological proximity rather than generic and abstract language. Our evidence suggests that following these guidelines will lead to more effective fear appeals. Using these guidelines, fear-appeal researchers can craft better experimental manipulations and practitioners can build more effective interventions.

Finally, we provide further evidence of fear appeals' potential to influence ISec-related behaviors. Few studies have reported such evidence in the ISec domain [e.g., 9, 77], perhaps because of the difficulty of observing behavior in this setting. Our discussion of the requirements for research designs that study behavioral outcomes, as well as our operationalization of such research designs, may inform future research seeking to include observed behaviors in their research designs. If researchers do this, it will improve the ability of the ISec literature to examine the effects of fear appeals on appraisal and behaviors.

Limitations and future research

Our research has several limitations that provide compelling research opportunities. *First*, is possible that the participants in Study 2 evaluated the spear phishing threat as primarily a threat to themselves and not to their organization. Although we took steps to construct clear and unequivocal fear-appeal treatments that were communicated by the CISO's office, some participants may have responded as they would have in a personal context. This was unavoidable, as we needed virtually perfect invariance in our research design to compare the results from Studies 1 and 2 and thus could not change the treatments. Because this is the first study to report such evidence, we encourage future research to corroborate these findings with evidence from modified research designs. The conundrum here is that all major fear-appeals research and theories insist that for a proper threat-appraisal process to occur, the threat must be personally relevant. Thus, it would be

Table 10. Theory- and evidence-based guidelines for designing more effective ISec fear appeals.

Guideline	Description	Examples (+ = positive, do this; - = negative, do not do this)
1. Depict fear appeals concretely (show, do not tell).	Focus on how instead of why: Illustrate the threat with detail and give examples.	***Explain how the threat puts recipients at risk* (+)**: "How does spear phishing work? It begins with a new email in your inbox that claims to be from a well-known brand, such as Wells Fargo, but is in fact from a criminal. It will typically look genuine and feature your name, a catchy subject line, and so on." ***Instead of generically saying why a threat is a dangerous* (-)**: "Why is spear phishing dangerous? It is deceptive because it attempts to trick victims into disclosing their information."
2. Specify concrete negative consequences.	Use vivid examples to show how the threat leads to negative consequences.	***Explain how the threat leads to concrete negative consequences* (+)**: "Once you click the link in the email, the criminal will have access to your personal information, and he/she can wreak havoc on your finances and reputation. Consider these examples: The criminal uses your information to buy goods with your credit card, borrow money under your name, or disseminate child pornography using elements of your web identity, such as your social media or email address." ***Instead of naming general negative consequences*** (-): "After the criminal gains access to private information, the consequences are often severe and typically affect finances and reputation."
3. Specify a concrete response procedure.	Clearly describe the steps that must be taken to protect against the threat.	***Explain how the concrete response is performed and helps mitigate the threat* (+)**: "In the first step, you need to learn the common clues that distinguish spear-phishing attacks. There are several clues that will indicate that the email is bogus. One example is the use of a forged sender's email address. Sometimes criminals will forge a look-a-like address from which they send the email to conceal its true origin. A first key step here is to always be aware of the identity and emails of important people and organizations you routinely correspond with via email. Everything else should be treated with heightened suspicion." ***Instead of giving generic mitigation advice*** (-): "Identifying spear-phishing attacks can be easily done by learning the common cues that typically reveal spear-phishing emails. Look out for anything suspicious!"
4. Convey psychological proximity.	Convey that a threat/response is proximate temporally, socially, spatially, and hypothetically.	***Convey that the threat is proximate and an urgent response is needed* (+)**: "For you, in your current environment, spear phishing is a realistic and likely threat—one that, statistically speaking, has already affected you and will affect you again soon. Thus, learning how to avoid spear phishing attacks is something you need to urgently learn to do soon, or you will fall victim and may not even know it." ***Instead of using generic statements that convey distal threats/responses*** (-): "This means, in general, that all Internet users are potentially endangered by spear phishing attacks. Thus, all Internet users around the world need to learn how to prevent spear phishing attacks."

Notes: The examples are modified from the manipulations used in Study 1 and Study 2. Although our findings on specifying concrete responses were not as conclusive over the course of three studies, we include them here because our theory applies in principle to the threat and response portion of a fear appeal.

particularly useful for employees to perceive spear phishing attempts in their organizations as personal threats, but this could lead to some unintended negative consequences for other security efforts that employees may view more as organizational threats that have little personal relevance.

Second, although this study was contextualized to an actual organization, the results may not generalize to all organizations. Although academic institutions have been used extensively in prior ISec organizational research [e.g., 15], the corresponding results may not apply well to for-profit organizations. Thus, organizational type is another contextual variation that should be considered in future research. As a related contextual consideration, previous ISec PMT research that did not use fear appeals found that employees with higher organizational commitment experienced higher threat, efficacy, and protection motivations than those with lower organizational commitment [77]. Recent research has also shown that other positive and negative emotions, aside from fear, can also influence employees' security behaviors [11, 20]. Thus, more contextualized construals research should be conducted that considers other emotions involved in threat and coping responses and other personal and organizational contextual factors, such as organizational type or organizational commitment.

Third, aside from considering the organizational context, there is a need to examine the utility of CLT-based fear appeals in additional ISec contexts. For instance, research claims that individuals typically become habituated to information-system security warnings and disregard them [97]. CLT could enable researchers to determine whether concrete security warnings in conjunction with specified concrete responses are more effective in gaining the attention of habituated users. For example, in the healthcare literature, which typically uses concrete fear appeals, such concrete messages have been shown to prevent users from becoming habituated due to frequent exposure [21]. We believe that a similar line of research would be especially useful for the ISec practice that seeks to keep users from habitually ignoring security warnings. This is also where ISec fear-appeals researchers may be too focused on PMT, given that an alternative theory, the extended parallel process model (EPMM), is available that explains both adaptive and maladaptive responses in parallel [105-107]. The EPPM could thus be more effective in dealing with a habituation context and other contexts where negative outcomes are common.

Fourth, although our evidence supports the conclusion that concrete fear appeals are more efficacious than abstract fear appeals in stimulating threat perceptions, our findings on the effects of response perceptions were not as conclusive. That said, this might be a confound from our context, because we studied a simple behavior; thus, further efficacy considerations may not have been a highly important factor for performing the desired response in our context. Moreover, threat appraisal and response appraisal involve different cognitive mechanisms and the coping appraisal may be more complex in organizational settings because of competing roles and organizational demands that can undermine efficacy and increase response costs. This would be especially relevant for desired security responses that are more time-intensive and complex. Thus, we surmise that more work needs to be done to develop principles for crafting fear appeals that raise efficacy under different levels of behavioral response complexity and when the behavioral response may be in conflict with an employee's traditional role.

Although we show strong empirical evidence of contextual differences between personal and organizational context, some of the contextual differences might be explained by

differences between our sample populations. Our sample populations differed in terms of prior training, frequency of phishing alerts received, and personal experience with phishing victimization (see Supplemental Online Appendix Table 3.8). Other studies have also identified further isolated other organizational factors that appear to matter (e.g., organizational commitment, workplace environment). Consequently, we suggest that more in-depth future research and theorization should be conducted to further examine contextual differences in organizations versus contextual differences in employees.

Another research opportunity is leveraging CLT to contextualize a wider range of security measures employed by organizations. A CLT perspective could help managers understand how users react to being informed of potential threats to organizations through, for example, "red hat" training exercises or actual "black hat" incursions. For instance, although many security organizations provide technical solutions that provide threat visualizations to cybersecurity departments, these systems simply point out potential cyberattacks without contextualizing them to the client's organization. Research needs to examine whether tools become more effective as they grow more apt at presenting concrete or abstract ISec messages to employees, be they expert IT personnel or part of the more general employee population. Moreover, the most sophisticated organizations have moved to carefully coordinated cyberthreat-intelligence initiatives (CTI) that not only examine threats comprehensively but use also advance intelligence to predict and thwart potential unknown threats [86]. No one has offered strong behavioral solutions that couple with CTI, and construals could be part of the answer. Such research could offer additional insights into how to help cybersecurity departments prioritize, identify, and combat complex cyberattacks.

Conclusion

We examined whether context and message abstractness could explain the mixed findings across the ISec literature. Although extant research has speculated that organizational contexts reduce the effects of fear appeals, we found that fear appeals lead to higher levels of fear and protection motivation among organizational users. We conclude that differences in context alone cannot account for the mixed findings among ISec fear-appeal studies and found significant effects related to the degree of message abstractness, with concrete fear-appeal messages being most effective. Thus, message abstractness helps to explain some of the conflicting findings in the previous literature, which has often relied on either no or weak (abstract) fear appeals. Our study provides evidence of the importance of crafting concrete fear appeals and offers specific guidance on how to do so.

Notes

1. CLT has been applied sparsely in business research, with limited applications in information systems (IS), management [7], and marketing [35]. In IS, a few studies have applied CLT to recommendation systems [55, 87], adoption [103], user innovation [51], or online forums [75].
2. For example, an abstract construal would describe phishing attacks in generic terms (e.g., "phishing is dangerous"), whereas a concrete construal would describe the danger of a phishing attack in more specific terms (e.g., "phishing emails will often ask you for personal and risky information, such as your credit card information").

3. For example, an abstract construal would represent spear phishing with high-level features, such as "dangerous," which would help indicate why someone should avoid spear phishing. In contrast, a concrete construal would represent spear phishing with low-level features, such as "requests your credit card information," which would indicate how one can avoid spear phishing—thus increasing the recipient's beliefs about their ability to detect phishing.
4. These are not the actual manipulations but example statements using the wording (i.e., linguistics) of the manipulations to illustrate their logic. The actual manipulations can be found in Supplemental Online Appendix 2.
5. The response part of each fear appeal was designed to be consistent with the threat manipulation. We tested a possible confounding effect of these abstract or concrete response videos using separate manipulation checks but did not find any significant effect on participants' threat perceptions or other dependent variables.
6. $\eta^2 \geq 0.06$ is considered a medium effect size and $\eta^2 \geq 0.14$ a large effect size. The following covariates were significant: Participants' protection motivation was significantly affected by media exposure ($p = 0.00$), previous phishing alerts received ($p = 0.01$), age ($p = 0.00$), and computer experience ($p = 0.02$). Threat severity was affected by computer self-efficacy ($p = 0.01$), and fear by gender ($p = 0.04$).
7. $\eta^2 \geq 0.06$ is considered a medium effect size. The following covariates had significant effects on PMT variables: Participants' protection motivation was affected by their weekly time spent reading about products and services on the Internet ($p = 0.00$) and their media exposure ($p = 0.00$). Threat severity significantly covaried with participants' weekly time spent reading about products and services on the Internet ($p = 0.03$). Fear was affected by participants' media exposure ($p = 0.02$). Participants' prior experience with phishing emails affected response cost perceptions ($p = 0.05$).
8. See the following blog post: https://blog.turkprime.com/after-the-bot-scare-understanding-whats-been-happening-with-data-collection-on-mturk-and-how-to-stop-it
9. For a discussion of how questions can influence participants' responses, see Perdue and Summers [74].
10. $\eta^2 \geq 0.06$ is considered a medium effect size and $\eta^2 \geq 0.14$ a large effect size. The following covariates were significant: Gender affected threat severity ($p = 0.02$), response efficacy ($p = 0.02$), and maladaptive rewards ($p = 0.04$). Age affected response cost ($p = 0.03$). Education affected response cost ($p = 0.01$) and response efficacy ($p = 0.03$). Job in IT affected fear ($p = 0.02$). Web experience affected protection motivation ($p = 0.01$). Risk affected threat severity ($p = 0.03$), response cost ($p = 0.02$), and maladaptive rewards ($p = 0.00$). Finally, computer self-efficacy affected threat severity ($p = 0.01$), maladaptive rewards ($p = 0.01$), protection motivation ($p = 0.03$), response cost ($p = 0.00$), self-efficacy ($p = 0.00$), and response efficacy ($p = 0.00$).
11. We present the logit, odds, probabilities, and marginal effects for interpretation of the results of binary logistic regression. Specifically, we follow past recommendations using binary logistic regression indicating that the marginal effects allow for better interpretation of the beta coefficient [37, 45, 108], as odd are often misinterpreted [52, 71]. Due to the use of the logistic function, the predictor variable does not have a consistent linear effect on the predicting variable and the relationship variable is dependent on the other predictor variables [37]. Accordingly, the marginal effect allows us to isolate the relationship and interpret the discrete change in probabilities from the treatment while assuming the other predictor variables are not present.

References

1. Alvesson, M.; and Karreman, D. Constructing mystery: Empirical matters in theory development. *Academy of Management Review*, *32*, 4 (2007), 1265–1281.
2. Anwar, M.; He, W.; Ash, I.; Yuan, X.H.; Li, L.; and Xu, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, April (2017), 437–443.

3. Bamberger, P. From the editors: Beyond contextualization—Using context theories to narrow the micro-macro gap in management research. *Academy of Management Journal*, *51*, 5 (2008), 839–846.
4. Bar-Anan, Y.; Liberman, N.; and Trope, Y. The association between psychological distance and construal level: Evidence from an implicit association test. *Journal of Experimental Psychology*, 135, 4 (2006), 609–622.
5. Bartnes, M.; Brede, N.; and Heegaard, P.E. The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, August (2016), 32–45.
6. Beitelspacher, L.S.; Hansen, J.D.; Johnston, A.C.; and Deitz, G.D. Exploring consumer privacy concerns and RFID technology: The impact of fear appeals on consumer behaviors. *Journal of Marketing Theory and Practice*, *20*, 2 (2012), 147–159.
7. Berson, Y.; Halevy, N.; Shamir, B.; and Erez, M. Leading from different psychological distances: A construal-level perspective on vision communication, goal setting, and follower motivation. *Leadership Quarterly*, *26*, 2 (2014), 143–155.
8. Blythe, J.M.; and Coventry, L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, October (2018), 87–97.
9. Boss, S.R.; Galetta, D.F.; Lowry, P.B.; Moody, G.D.; and Polak, P. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly*, *39*, 4 (2015), 837–864.
10. Burns, A.J.; Roberts, T.L.; Posey, C.; and Lowry, P.B. Examining the influence of organisational insiders' psychological capital on information security threat and coping appraisals. *Computers in Human Behavior*, *68*, March (2017), 190–290.
11. Burns, A.J.; Roberts, T.L.; Posey, C.; and Lowry, P.B. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, *30*, 4 (2019), 1228–1247.
12. Burton-Jones, A.; and Gallivan, M.J. Toward a deeper understanding of system usage in organizations: A multilevel perspective. *MIS Quarterly*, *31*, 4 (2007), 657–679.
13. Busse, C.; Kach, A.P.; and Wagner, S.M. Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, *20*, 4 (2017), 574–609.
14. Cannon, J. Using construal level theory to promote HPV vaccine uptake among college males. In *School of Communication*, Master of Arts: Purdue University, 2016.
15. Chan, Y.E.; Sabherwal, R.; and Thatcher, J.B. Antecedents and outcomes of strategic IS alignment: an empirical investigation. *IEEE Transactions on Engineering Management*, *53*, 1 (2006), 27–47.
16. Chandran, S.; and Menon, G. When a day means more than a year: Effects of temporal framing on judgements of health risk. *Journal of Consumer Research*, *31*, 2 (2004), 375–389.
17. Chen, Y.; and Zahedi, F. Individual's Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40*, 1 (2016), 205–222.
18. Choi, Y.K.; Seo, Y.; and Yoon, S. E-WOM messaging on social media: social ties, temporal distance, and message concreteness. *Internet Research*, *27*, 3 (2017), IntR-07-2016-0198.
19. Corley, K.; and Gioia, D. Building theory about theory building: What constitutes a theoretical contribution? *Academy of Management Review*, *36*, 1 (2011), 12–32.
20. D'Arcy, J.; and Lowry, P.B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*, 1 (2019), 43–69.
21. Dijkstra, A.; and Bos, C. The effects of repeated exposure to graphic fear appeals on cigarette packages: A field experiment. *Psychology of Addictive Behaviors*, *29*, 1 (2015), 82–90.

22. Dillard, J.P.; Plotnick, C.A.; Godbold, L.C.; Freimuth, V.S.; and Edgar, T. The multiple affective outcomes of AIDS PSAs: Fear appeals do more than scare people. *Communication Research*, *23*, 1 (1996), 44–72.
23. Eyal, T.; Liberman, N.; and Trope, Y. The pros and cons of temporally near and distant action. *Journal of Personality and Social Psychology*, *86*, 6 (2004), 781–795.
24. Eyal, T.; Liberman, N.; and Trope, Y. Judging near and distant virtue and vice. *Journal of Experimental Social Psychology*, *44*, 4 (2008), 1204–1209.
25. Faul, F.; Erdfelder, E.; Lang, A-G.; and Buchner, A. G*Power 3: A flexible statistical power analysis program for the social, behavior and biomedical sciences. *Behavior Research Methods*, *39*, 2 (2007), 175–191.
26. Fiske, S.T.; and Taylor, S.E. *Social Cognition*, 2, revised ed. New York, NY: McGraw-Hill, 1991.
27. Floyd, D.L.; Prentice-Dunn, S.; and Rogers, R.W. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*, 2 (2000), 407–429.
28. Freitas, A.L.; Gollwitzer, P.M.; and Trope, Y. The influence of abstract and concrete mindsets on anticipating and guiding others' self-regulatory efforts. *Journal of Experimental Social Psychology*, *40*, (2004), 739–752.
29. Fujita, K.; Eyal, T.; Chaiken, S.; Trope, Y.; and Liberman, N. Influencing attitudes toward near and distant objects. *Journal of Experimental Social Psychology*, *44*, 3 (2008), 562–572.
30. Hair, J.; Hollingsworth, C.L.; Randolph, A.B.; and Chong, A. An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, *117*, 3 (2017), 442–458.
31. Han, D; Duhachek, A; and Agrawal, N. Coping and construal level matching drives health message effectiveness via response efficacy or self-efficacy enhancement. *Journal of Consumer Research*, *43*, 3 (2016), 429–447.
32. Hansen, J.; and Wänke, M. Truth from language and truth from fit: the impact of linguistic concreteness and level of construal on subjective truth. *Personality and Social Psychology Bulletin*, *36*, 11 (2010), 1576–1588.
33. Henseler, J.; Ringle, C.M.; and Sarstedt, M. Testing measurement invariance of composites using partial least squares. *International Marketing Review*, *33*, 3 (2016), 405–431.
34. Herath, T.; and Rao, H.R. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 2 (2009), 106–125.
35. Hernandez, J.M.D.C.; Wright, S.A.; and Rodrigues, F.F. Attributes versus benefits: The role of construal levels and appeal type on the persuasiveness of marketing messages. *Journal of Advertising*, *44*, 3 (2014), 1–11.
36. Hina, S.; Durai, D.; and Lowry, P.B. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, November (2019), Article 101594.
37. Hoetker, G. The use of logit and probit models in strategic management research: Critical issues. *Strategic Management Journal*, *28*, 4 (2007), 331–343.
38. Hong, J. The current state of phishing attacks. *Communications of the ACM*, *55*, 1 (2012), 74–81.
39. Hong, W.; Chan, F.K.Y.; Thong, J.Y.L.; Chasalow, L.C.; and Dhillon, G. A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*, 1 (2014), 111–136.
40. Horton, J.J.; Rand, D.G.; and Zeckhauser, R.J. The online laboratory: Conducting experiments in a real labor market. *Experimental Economics*, *14*, 3 (2011), 399–425.
41. Hosmer, D.W.; and Lemeshow, S. *Applied Logistic Regression*. New York: Wiley, 2013.
42. Huang, N.; Burtch, G.; Hong, Y.; and Polman, E. Effects of multiple psychological distances on construal level: A Field study of online reviews. *Journal of Consumer Psychology*, *26*, 4 (2016), 474–482.

43. Hull, D.M.; Lowry, P.B.; Gaskin, J.E.; and Mirkovski, K. A storyteller's guide to problem-based learning for information systems management education. *Information Systems Journal*, *29*, 5 (2019), 1040–1057.
44. Jagatic, T.N.; Johnson, N.A.; Jakobsson, M.; and Menczer, F. Social phishing. *Communications of the ACM*, *50*, 10 (2007), 94–100.
45. Jensen, M.L.; Dinger, M.; Wright, R.T.; and Thatcher, J. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*, 2 (2017), 597–626.
46. Johns, G. The essential impact of context on organizational behavior. *Academy of Management Review*, *32*, 2 (2006), 386–408.
47. Johnston, A.C.; and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*, 3 (2010), 549–566.
48. Johnston, A.C.; Warkentin, M.; Dennis, A.R.; and Siponen, M. Speaking their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*, 2 (2019), 245–284.
49. Johnston, A.C.; Warkentin, M.; McBride, M.; and Carter, L. Dispositional and situational factors: influences on information security policy violations. *EJIS*, *25*, 3 (2016), 231–251.
50. Johnston, A.C.; Warkentin, M.; and Siponen, M. An enhanced fear appeal rethorical framework: Leveraging threats to the human asset through sanctioning rethoric. *MIS Quarterly*, *39*, 1 (2015), 113–134.
51. Kankanhalli, A.; Ye, H.; and Teo, H.H. Comparing potential and actual innovators: An empirical study of mobile data services innovation. *MIS Quarterly*, *39*, 3 (2015), 667–682.
52. Kaufman, R.L. Comparing effects in dichotomous logistic regression: A variety of standardized coefficients. *Social Science Quarterly*, *77*, 1 (1996), 90–109.
53. Kim, K.; and Kim, H-S. Time matters: Framing antismoking messages using current smokers' preexisting perceptions of temporal distance to smoking-related health risks. *Health Communication*, *33*, 3 (2018), 338–348.
54. Klohn, L.S.; and Rogers, R.W. Dimensions of the severity of a health threat: The persuasive effects of visibility, time of onset, and rate of onset on young women's intentions to prevent osteoporosis. *Health Psychology*, *10*, 5 (1991), 323–329.
55. Köhler, C.F.; Breugelmans, E.; and Dellaert, B.G.C. Consumer acceptance of recommendations by interactive decision aids: The joint role of temporal distance and concrete versus abstract communications. *Journal of Management Information Systems*, *27*, 4 (2011), 231–260.
56. Kumaraguru, P.; Sheng, S.; Acquisti, A.; Cranor, L.F.; and Hong, J. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*, 2 (2010), 1–31.
57. Liberman, N.; and Förster, J. Distancing from experienced self: how global-versus-local perception affects estimation of psychological distance. *Journal of Personality and Social Psychology*, *97*, 2 (2009), 203–216.
58. Lowry, P.B.; D'Arcy, J.; Hammer, B.; and Moody, G.D. "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *Journal of Strategic Information Systems*, *25*, 3 (2016), 232–240.
59. Lowry, P.B.; Dinev, T.; and Willison, R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, *26*, 6 (2017), 546–563.
60. Lutchyn, Y.; and Yzer, M. Construal level theory and theory of planned behavior: Time frame effects on salient belief generation. *Journal of Health Communication*, *16*, 6 (2011), 595–606.
61. MacKenzie, S.B.; Podsakoff, P.M.; and Podsakoff, N.P. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*, 2 (2011), 293–334.
62. Maddux, J.E.; and Rogers, R.W. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*, 5 (1983), 469–479.

63. Malhotra, N.K.; Kim, S.S.; and Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*, 4 (2004), 336–355.
64. Marett, K.; McNab, A.L.; and Harris, R.B. Social networking websites and posting personal information: An evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interactions*, *3*, 3 (2011), 170–188.
65. Mason, W.; and Suri, S. Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, *44*, 1 (2012), 1–23.
66. Menard, P.; Bott, G.J.; and Crossler, R.E. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*, 4 (2017), 1203–1230.
67. Menard, P.; Warkentin, M.; and Lowry, P.B. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, June (2018), 147–166.
68. Milne, S.; Sheeran, P.; and Orbell, S. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*, 1 (2000), 106–143.
69. Nan, X. Social distance, framing, and judgment: A construal level perspective. *Human Communication Research*, *33*, 4 (2007), 489–514.
70. Niederman, F.; and March, S. Reflections on replications. *AIS Transactions on Replication Research*, *1*, 4 (2015), 1–16.
71. Norton, E.C.; Wang, H.; and Ai, C. Computing interaction effects and standard errors in logit and probit models. *The Stata Journal*, *4*, 2 (2004), 154–167.
72. Paolacci, G.; Chandler, J.; and Ipeirotis, P. Running experiments on amazon mechanical turk. *Judgment and Decision Making*, *5*, 5 (2010), 411–419.
73. Peng, C-Y.J.; Lee, K.L.; and Ingersoll, G.M. An introduction to logistic regression analysis and reporting. *The Journal of Educational Research*, *96*, 1 (2002), 1–14.
74. Perdue, B.C.; and Summers, J.O. Checking the success of manipulations in marketing experiments. *Journal of Marketing Research*, *23*, 4 (1986), 317–326.
75. Phang, C.W.; Kankanhalli, A.; and Tan, B.C.Y. What motivates contributors vs. lurkers? An investigation of online feedback forums. *Information Systems Research*, *26*, 4 (2015), 773–792.
76. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J-Y.; and Podsakoff, N.P. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*, 5 (2003), 879–903.
77. Posey, C.; Roberts, T.L.; and Lowry, P.B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*, 4 (2015), 179–214.
78. Puhakainen, P.; and Siponen, M. Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*, 4 (2010), 757–778.
79. Rhee, H-S.S.; Kim, C.; and Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*, 8 (2009), 816–826.
80. Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*, 1 (1975), 93–114.
81. Rogers, R.W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 19. New York, NY: Guilford Press, 1983, pp. 153–176.
82. Rogers, R.W.; and Prentice-Dunn, S. Protection motivation theory. In D.S. Gochman (ed.), *Handbook of Health Behavior Research I: Personal and Social Determinants*. New York, NY: Plenum Press, 1997, pp. 113–132.
83. Rohm, A.J.; and Milne, G.R. Just what the doctor ordered. The role of information sensitivity and trust in reducing medical information privacy concern. *J. of Business Research*, *57*, 9 (2004), 1000–1011.

84. Semin, G.R.; Higgins, T.; de Montes, L.G.; Estourget, Y.; and Valencia, J.F. Linguistic signatures of regulatory focus: How abstraction fits promotion more than prevention. *Journal of Personality and Social Psychology*, *89*, 1 (2005), 36–45.
85. Shewan, D. How much does Google ads cost?, 2019. https://www.wordstream.com/blog/ws/2015/05/21/how-much-does-adwords-cost (accessed September 1, 2019).
86. Shin, B.; and Lowry, P.B. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, *92*, May (2020), Article 101761.
87. Shmueli, L.; Benbasat, I.; and Cenfetelli, R.T. A construal-level approach to persuasion by personalization. Presented at *International Conference of Information Systems*, Dublin, Ireland, pp. 1–19.
88. Silic, M.; and Lowry, P.B. Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*, 1 (2020), 129–161.
89. Siponen, M. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*, 1 (2000), 31–41.
90. Smith, E.R. Mental representation and memory. In D.T. Gilbert, S.T. Fiske, and G. Lindzey (eds.), *The Handbook of Social Psychology*, 1. New York, NY: McGraw-Hill, 1998, pp. 391–445.
91. Steelman, Z.R.; Hammer, B.I.; and Limayem, M. Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, *38*, 2 (2014), 355–378.
92. Steidle, A.; Werth, L.; and Hanke, E.V. You can't see much in the dark: Darkness affects construal level and psychological distance. *Social Psychology*, *42*, 3 (2011), 174–184.
93. Stephan, E.; Liberman, N.; and Trope, Y. The effects of time perspective and level of construal on social distance. *Journal of Experimental Social Psychology*, *47*, (2011), 397–402.
94. Sutton, S.R. Fear-arousing communications: A critical examination of theory and research. *Social Psychology and Behavioral Medicine*, *1982*, (1982), 303–337.
95. Tannenbaum, M.B.; Hepler, J.; Zimmerman, R.S.; Saul, L.; Jacobs, S.; Wilson, K.; and Albarracín, D. Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychiatric Bulletin*, *141*, 6 (2015), 1178–1204.
96. Trope, Y.; and Liberman, N. Construal-level theory of psychological distance. *Psychological Review*, *117*, 2 (2010), 440–463.
97. Vance, A.; Jenkins, J.L.; Anderson, B.B.; Bjornn, D.K.; and Kirwan, C.B. Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly*, *32*, 2 (2018), 1–XX.
98. Wall, J.D.; and Buche, M.W. To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*, 13 (2017), 277–300.
99. Wang, J.; Herath, T.; Chen, R.; Vishwanath, A.; and Rao, H.R. Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*, 4 (2012), 345–362.
100. Wang, J.; Li, Y.; and Rao, H.R. Coping responses in phishing detection: An Investigation of antecedents and consequences. *Information Systems Research*, *28*, 2 (2017), 378–396.
101. Warkentin, M.; Walden, E.A.; Johnston, A.C.; and Straub, D.W. Neural correlates of protection motivation for secure IT behaviors: An fMRI exploration. *Journal of the Association for Information Systems*, *17*, 3 (2016), 194–215.
102. White, K.; MacDonnell, R.; and Dahl, D.W. It's the mind-set that matters: The role of construal level and message framing in influencing consumer efficacy and conservation behaviors. *Journal of Marketing Research*, *48*, June (2011), 472–485.
103. White, T.B.; Novak, T.P.; and Hoffman, D.L. No strings attached: When giving it away versus making them pay reduces consumer information disclosure. *J. of Interactive Marketing*, *28*, 3 (2014), 184–195.
104. Williams, L.E.; Stein, R.; and Galguera, L. The distinct affective consequences of psychological distance and construal level. *Journal of Consumer Research*, *40*, 6 (2014), 1123–1138.

105. Witte, K. Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*, 4 (1992), 329–349.
106. Witte, K. Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs*, *61*, 2 (1994), 113–134.
107. Witte, K.; and Allen, M. A meta-analysis of fear appeals. *Health Education & Behavior*, 27, 5 (2000), 591–615.
108. Wright, R.T.; Jensen, M.L.; Thatcher, J.B.; Dinger, M.; and Marett, K. Influence techniques in phishing attacks: An examination of vulnerability and resistance. *ISR*, *25*, 2 (2014), 385–400.
109. Wright, R.T.; and Marett, K. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *J. of Management Information Systems*, *27*, 1 (2010), 273–303.
110. Yu, A. Elaborate phishing scams increasingly target universities, 2019. https://whyy.org/articles/elaborate-phishing-scams-increasingly-target-universities/(accessed September 1, 2019).

About the Authors

Sebastian W. Schuetz is an Assistant Professor at Florida International University. He received his Ph.D. in Information systems from the City University of Hong Kong in 2017. His research interests relate to information security management and the societal implications of information technology. His work has appeared, among others, in the *Journal of Management Information Systems, Journal of the AIS, Information Systems Journal*, and several international conferences.

Paul Benjamin Lowry is the Suzanne Parker Thornhill Chair Professor and Eminent Scholar at the Pamplin College of Business at Virginia Tech. He is also the BIT Ph.D. program director. He received his Ph.D. in Management Information Systems from the University of Arizona. His research interests include organizational and behavioral security and privacy; online deviance, online harassment, and computer ethics; human-computer interaction, social media, and gamification; and business analytics, decision sciences, innovation, and supply chains. Dr. Lowry has published over 127 papers in the *Journal of Management Information Systems* (*JMIS*), *MIS Quarterly, Information Systems Research, Journal of the AIS (JAIS), Information System Journal (ISJ), European Journal of Information Systems*, and others. He is a member of the Editorial Board of *JMIS*, a department editor of *Decision Sciences*, and senior editor of *JAIS* and *ISJ*.

Daniel A. Pienta is an Assistant Professor at Baylor University. He received his Ph.D. in Information Systems from Clemson University. His research focuses on behavioral and technical cybersecurity. He has worked as the managing director of a cybersecurity and due diligence consulting firm, specialized in servicing some of the largest commercial lending institutions. He has extensive experience in penetration testing, information system design and development, and user experience. His work has appeared or is forthcoming in *Journal of Management Information Systems, Journal of Information Technology, Communications of the AIS*, and the proceedings of several international conferences.

Jason Bennett Thatcher holds the Milton F. Stauffer Professorship in the Department of Management Information Systems at the Fox School of Business of Temple University. Dr. Thatcher's research examines the influence of individual beliefs and characteristics on technology use, cybersecurity, and IT human resource management in organizations. His work appears in the *Journal of Management Information Systems, MIS Quarterly, Information Systems Research, Journal of Applied Psychology, Organizational Behavior and Human Decision Processes*, and *Journal of the AIS*. He has served as President of the Association for Information Systems and Senior Editor at *MIS Quarterly*.