EUROPEAN JOURNAL OF INFORMATION SYSTEMS
2021, VOL. 30, NO. 1, 27–45
https://doi.org/10.1080/0960085X.2020.1793696

THE OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

EMPIRICAL RESEARCH

Using susceptibility claims to motivate behaviour change in IT security

Matthew L. Jensen[a], Alexandra Durcikova[a] and Ryan T Wright[b]

[a]MIS Division, Price College of Business, University of Oklahoma, Norman, USA; [b]McIntire School of Commerce, University of Virginia, Charlottesville, USA

ABSTRACT

Organisations face growing IT security risks with substantial consequences for missteps in business continuity, data loss, reputational harm, and future competitive advantage. To improve precaution-taking among organisation members, leaders frequently turn to susceptibility claims embedded in security education, training, and awareness (SETA) initiatives to motivate change. However, prior studies have produced mixed empirical results concerning the role of susceptibility in motivating precaution-taking. To deepen theorising about using susceptibility claims to change behaviour, we argue that threat characteristics (overt versus furtive attacks) shape individuals' attitudes of the threat, and these attitudes subsequently anchor how individuals respond to new claims about the threats. We introduce social judgement theory (SJT) to argue that when individuals participate in SETA initiatives, susceptibility claims that are too distant from individuals' existing attitudes will be ignored, while claims that are more proximal are more likely to be accepted and result in behaviour change. Using a longitudinal field experiment, we found that susceptibility claims motivated precaution taking against phishing (overt attack) but did not against password cracking (furtive attack). These results support SJT predictions and imply latitudes of acceptability and rejection into which susceptibility claims are placed. Implications for researchers, organisation leaders, and SETA developers are discussed.

ARTICLE HISTORY
Received 18 May 2018
Accepted 3 July 2020

ACCEPTING EDITOR
Dov Te'eni

ASSOCIATE EDITOR
Anat Hovav

KEYWORDS
Phishing; password; susceptibility; fear appeal; field experiment; social judgement theory; overt attack; furtive attack; latitude of acceptability; latitude of rejection

1. Introduction

National and international headlines are littered with news stories about organisations that have suffered embarrassing data breaches (e.g., Airbus; Corfield, 2019), digital thefts (e.g., 500,000 USD of city employees' paychecks rerouted; Etters, 2019), digital extortion (e.g., UK Police Federation ransomware attack; Martin, 2019), or loss of intellectual property (48% UK manufacturers under attack; Ashford, 2018). The potential consequences of cyber threats extend beyond substantial financial losses to include interruptions to business continuity, loss of data, reputational harm, reduction of future competitive advantage, and ill will from partners and customers. Boards of public companies are increasingly scrutinising management decisions concerning digital safeguards and failures in IT security are now grounds for dismissing senior executives (Basu, 2014). Therefore, IT security is rising among organisational priorities. According to Gartner (Gartner, 2018), organisations are expected to spend 124 USD billion in 2019 on information security, an 12.4% increase from 2018, with the priority on preventative security measures. Additionally, employees are increasingly being asked to assume a more active role in protecting organisations' digital assets (Givens, 2019).

To reduce their exposure to cyber threats and increase the IT security capabilities of their organisations, leaders invest in security education, training, and awareness (SETA) initiatives with the specific goal of building employees' awareness and resilience to cyberattacks. For example, many organisations require employees to complete annual IT security training addressing organisational threats such as phishing, password security, and other cyber-hygiene topics. In fact, legislation (e.g., General Data Protection Regulation in the European Union, Health Insurance Portability, and Accountability Act in the United States, etc.) mandates cybersecurity training for employees who handle sensitive data and government bodies (e.g., National Institute of Standards and Technology in the United States) provides guidelines for keeping unregulated data safe. Past research has demonstrated that SETA initiatives can have a significant effect on improving IT security capabilities within organisations (e.g., Pattabiraman et al., 2018; Puhakainen & Siponen, 2010). Therefore, some IT security leaders have argued that SETA initiatives are among the best cybersecurity investments (Disparte & Furlow, 2017).

In SETA initiatives, fear appeals are commonly used to persuade organisation members to take protective action (Johnston & Warkentin, 2010). Specifically, individuals learn about the negative consequences that may occur if they do not comply with the guidelines in the SETA initiative, and the desire to avoid these negative consequences is thought to motivate behaviour change. A principal component

CONTACT Ryan T Wright ✉ rtw2n@virginia.edu

of behaviour-changing fear appeals is perceived susceptibility to the threat. *Threat susceptibility* is the likelihood that a threat will be realised and an individual will experience the negative consequences associated with the threat (Rogers, 1975). For example, threat susceptibility is made salient in SETA initiatives using claims describing the frequency an individual will experience a threat or certainty of a threat being realised against an individual (Witte, 1992). Although using susceptibility to motivate behaviour change seems intuitive, susceptibility claims in SETA initiatives have produced mixed empirical support (see Appendix A for a review). For instance, some research demonstrates improvement in IT security intentions and behaviour resulting from high susceptibility claims (Anderson & Agarwal, 2010; Boss et al., 2015), but others report little or no change in behaviour (Crossler, 2010; Herath & Rao, 2009; Johnston & Warkentin, 2010). Researchers have suggested that this inconsistency may stem from poor specification and application of fear appeal and behaviour change theory (Boss et al., 2015), an overemphasis on intention and lack of focus on behaviour (Boss et al., 2015), or threats that lack personal relevance (Johnston et al., 2015).

We contribute to SETA research by exploring inconsistent findings regarding the impact of susceptibility claims on behaviour. We describe threat characteristics (e.g., overt attacks on persons) that influence individuals' attitudes about threats and govern their response to claims of threat susceptibility that are used to motivate precaution-taking behaviour. We argue that when SETA initiatives invoke threat susceptibility, individuals likely evaluate these claims against their existing attitudes towards the threat. If individuals' attitudes are congruent with susceptibility claims, the SETA initiative will be more likely to succeed in motivating behaviour change. For example, if individuals have noticed past overt attacks and believe they are prevalent, SETA campaigns claiming high susceptibility are likely to be credible and will promote precaution taking. However, if individuals' existing attitudes are misaligned with susceptibility claims, the SETA campaign is unlikely to motivate behaviour change. Instead, the training is likely to be dismissed as irrelevant.

We extend past IT security research to account for the alignment between threat susceptibility claims and the characteristics of the threat by introducing social judgement theory (Sherif & Hovland, 1961; Sherif et al., 1965) as an overarching explanation for why past research on threat susceptibility is mixed. We describe the mechanism by which existing attitudes can anchor responses to new susceptibility claims and test these predictions with a longitudinal field experiment. Participants were directed to take precautions against two of the most common IT security threats (Solman, 2015). The first threat, password cracking, involved attacks that are largely *furtive* to the user. The second threat, phishing, involved *overt* attacks to which users must respond for the attack to be successful. Immediately following the training session, participants recorded their intentions to comply with the guidelines in the SETA initiative. Participants were later subjected to password cracking attacks and phishing attacks conducted by the organisation's IT security department. We then compared participants' intentions to comply with the guidance in the SETA initiative and their actual precaution-taking behaviour in response to susceptibility claims.

2. Theoretical development

In SETA initiatives, susceptibility claims are usually combined with other components of fear appeals designed to alter behaviour. According to Witte (1992), "fear appeals are persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" (pg. 329). Traditional fear appeals include two components: a description of the threat and a description of the action(s) individuals should take to mitigate the threat. The expected success of a fear appeal is determined by threat appraisals (e.g., threat susceptibility, severity, rewards of non-compliance) and coping appraisals (e.g., self-efficacy, response efficacy, cost of compliance), which combine to induce a maladaptive response (e.g., the continuance of risky behaviour) or an adaptive response (e.g., risk-mitigating behaviour change) (Bulgurcu et al., 2010; Rogers, 1975, 1983). For a fear appeal to induce an adaptive response, the coping appraisal must align with the threat appraisal to support a credible way to escape the threat. Fear appeals have been successfully used to encourage precaution-taking in applications such as cancer screening (Easterling & Leventhal, 1989), prevention of AIDS (LaTour & Pitts, 1989), seatbelt use (Lewis et al., 2007), prevention of smoking (Smith & Stutts, 2003), and even politics (De Castella et al., 2009).

Although threat susceptibility has been cast as a critical contributor to fear appeals (Rogers, 1975, 1983), the relationship between susceptibility claims and behaviour change has mixed empirical support, with significant variability in SETA initiatives in particular (see Appendix A for a systematic review of research on the role of susceptibility in SETA initiatives). For example, some researchers confirmed the findings uncovered outside of the IT domain: susceptibility claims increased intentions to comply with SETA initiatives and produced adaptive behaviour changes (e.g., Anderson & Agarwal, 2010; Boss et al., 2015). However, others report no change (Herath & Rao, 2009; Johnston & Warkentin, 2010) or found that susceptibility claims *reduced* precaution-taking behaviour (Crossler, 2010).

2.1. Challenges in using susceptibility for behaviour change

Several researchers (e.g., Wall & Buche, 2017) have noted the inconsistency in the relationship between susceptibility (among other aspects of fear appeals) and behaviour change and have postulated explanations for the variability. The explanations fall into two categories stemming from methodological and theoretical issues. First, methodological explanations for variability (e.g., Boss et al., 2015) have highlighted the prevalence of research on intentions to comply with a fear appeal instead of actual behaviour change. While self-reported intentions and behaviour often coincide when individuals interact with digital systems (e.g., A. C. Johnston et al., 2016; Vance et al., 2015), the relationship between intentions and behaviour has also been inconsistent (Limayem et al., 2007). This inconsistency has been especially prominent in IT security contexts where researchers have noted a conspicuous intention-behaviour gap (Crossler et al., 2014), even when the cost of compliance is very low (Acquisti & Grossklags, 2004). One estimate suggests that intentions alone account, on average, for only 28% of the variance in behaviour (Sheeran, 2002). As a result, IT researchers have called for an increase in attention paid to actual behaviour rather than only intentions and their antecedents (Boss et al., 2015; De Guinea & Markus, 2009).

Second, the theoretical explanations for variability in the relationship between susceptibility and behaviour change involve missing factors in theoretical models and misappropriation of referent theory. Researchers (e.g., Grover et al., 2008; Oswick et al., 2011; Truex et al., 2006) have noted that appropriation of theories from referent disciplines (e.g., communication, psychology) has yielded important advances for the IS discipline; however, research relying on referent theories occasionally neglects factors that are critical for the appropriate application. Traditional contexts for fear appeal applications (e.g., personal health and safety) are personally relevant to the majority of individuals targeted by the fear appeal. In fact, personal relevance is a core condition for the appropriate use of fear appeals (Slater, 2006). However, IT security researchers have suggested that guarding organisational information assets may not be seen as personally relevant as improving one's health or safety (Johnston et al., 2015; Moody et al., 2018) and that IT security appeals do not generate fear (Warkentin et al., 2016). Therefore, susceptibility claims may be less effective when employed to improve organisational protections because a core condition of the theory is not satisfied. As a result, some researchers have investigated the use of sanctions (Johnston et al., 2015; Kankanhalli et al., 2003; Pahnila et al., 2007; Siponen & Vance, 2010; Willison, Warkentin et al., 2018), anti-neutralisation techniques (Barlow et al., 2018), and deterrence (Willison, Lowry et al., 2018) to increase compliance with SETA campaigns with positive results.

Additionally, fear appeal theory describes behaviour *change* (Velicer & Prochaska, 2008). Typically, SETA campaign participants have existing attitudes and behaviours that the campaign must demonstrate as deficient and in need of change to be effective. Therefore, the decision of whether to adopt the practices advocated in SETA messaging precipitates a comparison between current and proposed practices. However, the implications of such comparisons are often not reflected in theorising the effects of susceptibility claims and fear appeals in general. For example, researchers have pointed out that the cost of compliance with security policy and rewards for non-compliance are often omitted from IT security studies. Yet these factors capture critical aspects of the comparison between current and proposed practices inherent in behaviour change (Boss et al., 2015; Bulgurcu et al., 2010).

These theoretical and methodological issues present an opportunity to deepen understanding regarding susceptibility claims and their effects in SETA initiatives. To address the theoretical issues concerning personal relevance and behaviour change, we introduce and build on social judgement theory (SJT; Sherif & Hovland, 1961; Sherif et al., 1965). Additionally, to address methodological issues, we tested our arguments in an ecologically valid field test that included the collection of intentions to follow SETA guidelines and actual security-related behaviours.

2.2. Susceptibility and social judgement

Determining susceptibility is highly salient during appraisal since it is often the gateway governing whether the threat deserves attentional resources and is followed by other components of threat appraisal (e.g., determination of severity) (Shah et al., 1999). Individuals have several sources of information upon which they may rely when estimating their susceptibility. Prior theorising relating to susceptibility has posited two potential sources of information (Tanner et al., 1991). As shown in Figure 1, the first source of information claims about susceptibility that is made in the message (e.g., in the SETA campaign), and previous research suggested that well-worded claims can improve protective behaviours (Johnston et al., 2019). The second source of information comes from the individual's existing attitudes, which are primarily based on direct, experiential, or observational learning (Taylor et al., 2005).

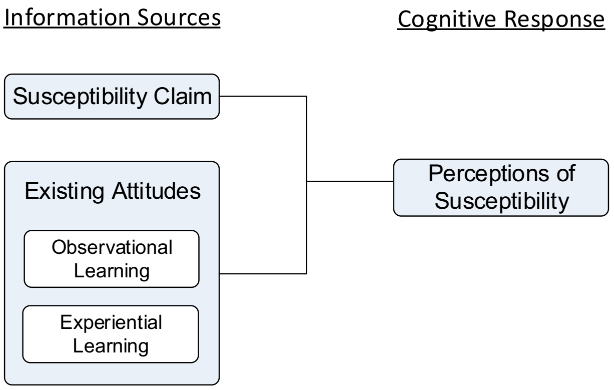

Figure 1. Information sources contributing to perceptions of susceptibility.

Ideally, claims and existing attitudes consistently portray threats so that individuals may accurately perceive their susceptibility. However, when information sources do not align, individuals must reconcile conflicting information sources in judging susceptibility.

SJT posits that when an individual encounters claims in persuasive messaging, the individual's existing attitudes will distort perceptions of the message and will mediate behaviour change (Sherif & Hovland, 1961; Sherif et al., 1965). For example, when a claim of susceptibility is made as part of a SETA campaign, individuals will reconcile this claim with their existing attitudes based on observational and experiential learning. During message evaluation, SJT predicts that individuals subconsciously form an evaluative continuum of beliefs divided into three segments: 1) latitude of acceptance, 2) latitude of non-commitment, and 3) latitude of rejection. As shown in Figure 2, claims within the latitude of acceptance and non-commitment are acceptable (New Claims A and B), while claims within the latitude of rejection are not acceptable (New Claim C). The location and size of each segment are determined by existing attitudes, which form a judgement standard or *anchor*.

Claims in persuasive messaging that are near the anchor (i.e., within latitudes of acceptance) are judged to be closer to existing attitudes than they actually are, and individuals assimilate their attitudes to include the new claims. For example, individuals may report that the claims in persuasive messaging already reflect their attitudes when they are close to their own attitudes, but not entirely aligned. Claims far from the anchor (i.e., within the latitude of rejection) are judged to be farther from existing attitudes than they actually are. Individuals contrast such claims from their attitudes, thus ignoring or derogating the message.

According to SJT, behaviour change is most likely to occur when persuasive messages are neither too close to the anchor (and presumably reflected in existing behaviour) nor too far from the anchor (and ignored or derogated) as is the case with New Claim B in Figure 2 (Sherif & Hovland, 1961; Sherif et al., 1965). SJT has explained attitude change in complex persuasive contexts such as increasing costs of higher education (Rhine & Severance, 1970), alcoholism reduction (Smith et al., 2006), legalisation of abortion (Sherif & Hovland, 1961), participation in armed conflict (Peterson & Koulack, 1969), thus demonstrating that existing attitudes are a powerful *internal* reference point[1] in the evaluation of persuasive messages.

2.3. Formation of susceptibility attitudes and threat characteristics

Since SJT predicts that existing attitudes form an important anchor for interpreting claims in persuasive messages, the way existing attitudes are formed represents a critical area of inquiry. The formation of susceptibility attitudes is especially crucial in IT security contexts because characteristics of IT security threats might alter the formation of these attitudes. Prior research has demonstrated that IT security threats have unique characteristics that influence subsequent protective behaviours (Belanger & Crossler, 2019; Posey et al., 2013). Likely, threat characteristics will also influence how individuals develop attitudes about them. For example, the types of threats listed in Table A1 (Appendix A) vary considerably, and the way individuals experience threats from violations of information security policy may be qualitatively different from how individuals experience threats from malware. Ignoring these characteristics diminishes an important

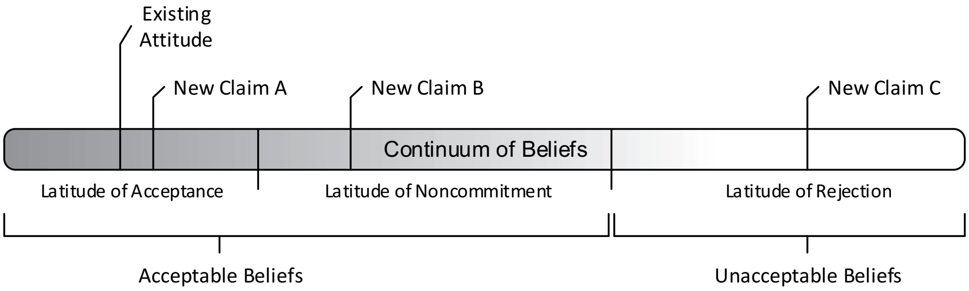

Figure 2. Examples of latitudes of acceptance, noncommitment, and rejection.

potential explanation for why susceptibility claims may fall into the latitudes of acceptance, noncommitment, or rejection and ultimately motivate behaviour change (or not).

To capture potential differences in how individuals experience and develop attitudes about IT security threats, we introduce a distinction between threats. *Overtness* is the degree to which individuals directly experience IT security threats and is derived from the perspective of the end user. Overtness is conceptualised as a continuum with threats that are furtive (or completely hidden from end users) on one side and those that are overt (or come into direct contact with end users) on the other side. On one hand, an example of an overt threat is phishing, which directly targets end users and against which users must take protective action. Although phishers are using deception to hide their nefarious purpose, end users can observe the attack as it unfolds, thus providing users with the firsthand experience about the attack and its potential consequences. On the other hand, an example of a furtive threat is password cracking which is largely hidden from end users, yet users still bear responsibility for taking protective action. Instead of attacking users directly, password crackers threaten other targets (e.g., organisational networks or systems) and avoid direct contact with end users in a way that prevents end users from directly observing the attack.

2.4. Hypotheses

To deepen theorising about susceptibility claims in IT security contexts, we argue that characteristics of IT threats themselves and the anchors of existing attitudes that these characteristics create combine to alter how susceptibility claims motivate behaviour change. Carvalho et al. (2008) found that personal relevance (as measured by the importance of the topic to the participant) moderates risk perceptions when an event is perceived to be likely to happen but does not have an effect when deemed unlikely to happen. Reyna and Farley (2006) suggest that individuals' evaluation of risk is influenced by specific information they have learned (e.g., prior attitudes) and a "fuzzy gist" representation, which captures psychological proximity to the risk (Teigen, 2005). Taken together, initial findings suggest that threat characteristics can shape attitudes about the threat and that together, threat characteristics and existing attitudes can govern behavioural responses.

In a similar vein, we argue that overt threats that come into direct contact with individuals will be more likely to produce higher anchors than furtive threats. The potential for direct contact with IT threats (e.g., as with a phishing email) provides evidence of susceptibility that may substantiate the legitimacy of the threat, increase its psychological proximity, and affect the placement of the anchor and latitudes which govern what is reasonable and not. Thus, threats that manifest through overt attacks should heavily influence existing attitudes and provide a salient internal anchor against which new claims are compared.

When organisation leaders use susceptibility claims in SETA initiatives, SJT predicts that participants will position those claims along their evaluative continuum of beliefs (i.e., Figure 2). Following the SETA instruction, participants will likely understand that organisation leaders believe the threat to be serious (and will know how to respond when asked later about how probable the threat is and how likely they are to change their behaviour). Participants may even be aware of potential sanctions that come from noncompliance with SETA guidelines. However, consistent with SJT, we anticipate that participant responses to susceptibility claims will be driven by participants' existing attitudes about the threat and the positioning of the claims in latitudes of acceptance, noncommitment, or rejection. On one hand, if participant attitudes are formed based on opaque, furtive attacks, high susceptibility claims invoked in SETA campaigns will likely be positioned in the latitude of rejection because the claims are too far from existing attitudes. The participants' internal anchor will overrule external claims, and the participants will likely respond maladaptively by ignoring or derogating the guidelines in the SETA campaign. On the other hand, if participant attitudes are formed based on direct experience with overt IT threats, high susceptibility claims will more likely be positioned in latitudes of acceptance or noncommitment. These claims are likely to be heeded, and if they are not too close so as to be assimilated, they will contribute to an adaptive response and legitimate behaviour change. Therefore, we propose the following[2]:

H1: Susceptibility claims will be more influential on intentions to take precautions for overt attacks than furtive attacks.

H2: Susceptibility claims will be more influential on precaution-taking behaviours for overt attacks than furtive attacks.

3. Method

In partnership with the IT security department of a large university in the United States, we developed a SETA initiative and manipulations that claimed high and low levels of threat susceptibility to password cracking (furtive attack) and phishing emails (overt attack). To test our hypotheses, we conducted two experiments. Experiment 1 (N = 136) checked participants' existing attitudes towards both types of threats and examined susceptibility claim manipulations that were included in the training. Experiment 2, a longitudinal field experiment (N = 138), examined the role of susceptibility claims in altering participants' intentions and actual performance of precaution-taking behaviour. Finally, we compared the effect of susceptibility claims for the password-cracking threat and the phishing threat.

This study design addressed the proposed explanations for the inconsistency between threat susceptibility and behaviour change. To rule out competing explanations due to other components of fear appeals (aside from susceptibility), we captured and included in statistical tests the contributors to threat appraisals (e.g., threat susceptibility, severity, rewards of non-compliance) and coping appraisals (e.g., self-efficacy, response efficacy, cost of compliance). We also gathered data about the helpfulness of the training to gauge personal relevance and explicitly accounted for comparisons between past and new requested practices in our empirical testing of SJT. Both experiments were conducted at the same university. However, participation in the experiments did not overlap. Both experiments and their results are discussed next in detail.

4. Experiment 1

4.1. Participants

Participants for experiment 1 were recruited from an introductory Management Information Systems class which is required for all business majors and several non-business majors. Participants were incentivised with a small amount of course credit (less than 1% of their final grade). A total of 158 participants began the study. However, 22 responses were discarded because participants provided incomplete responses, did not follow instructions, or failed attention check items. The remaining 136 comprised the experiment sample.

4.2. Training materials

The SETA initiative was introduced to participants as a training by the IT security department, which would inform them of IT security policies and elevate the level of cyber hygiene among faculty, staff, and students. Participants were shown a video containing a narrated slide show with accompanying subtitles. Instruction concerning password management and avoiding phishing attacks was included alongside instructions about proper online behaviour and protection of personally identifiable information (PII).

The guidelines in the training were developed based on best industry practices (Anti-Phishing Working Group, 2016; National Institute of Standards and Technology, 2016), prior research (Jensen et al., 2017; Kumaraguru et al., 2010; Wright et al., 2014), policies in place at the university, and government regulations. To ensure accessibility and utility, the content of the SETA initiative underwent several iterations of review and modification by employees and managers in the IT security department, a small group of university faculty, and local IT support personnel. The training highlighted the need to change their passwords if they were less than eight characters long or more than one-year old. The training also highlighted explicit guidance regarding steps participants should take if they receive a suspicious email (e.g., Never open an attachment or click on a link in a message from someone you don't know, Mouse over any embedded links to make sure they are what you expect). A summary of the instructional material regarding password management and avoiding phishing is provided in Appendix B. Following the training, participants agreed that the training was helpful to them across the covered areas (password management M = 4.18, SD =.70; avoiding phishing: M = 4.04, SD = .77).[3]

4.3. Manipulations

Characteristics of the threat (overt versus furtive) and level of susceptibility claimed (high versus low) constituted the primary manipulations of the experiments. Password cracking and phishing attacks were selected as threats because they are among the most common ways attackers breach organisational systems (Barrett, 2016; FBI, 2016; Verizon, 2017). Further, both types of attacks fall under *account protection* in Posey et al.'s (2013) taxonomy and therefore, share similar organisational risks. However, the threats differ in their level of direct contact with individuals.

Password cracking is now a common hacking technique (Savage, 2019) that is often propagated through network attacks (DUO, 2016), brute force attacks (Steinberg, 2016), and taking advantage of password reuse and past data breaches (Fitzgerald, 2016; Ives et al., 2004; Palfy, 2019). These attacks target organisation systems and are largely furtive to the user. However, phishing attacks overtly target and directly contact individuals. Therefore, as we argued above, individuals are likely to be more aware of phishing attacks against them. Consistent with this conceptual distinction between types of threats, participants in the pilot reported prior to the training that they experience more phishing attacks (M = 1.88, SD = .811) than password cracking attacks (M = 1.58, SD = .763; paired-t(95) = 3.542, p = .001).[4] Although participants reported rarely experiencing both types of attacks, the significant difference in existing attitudes between the threats has implications for how claims about the threats will be interpreted. According to SJT, the higher perceptions of phishing should confer a higher anchor and would adjust latitudes of acceptance, non-commitment, and rejection accordingly.

Susceptibility claims were shown prior to the delivery of the training content and were reinforced by repetition after the training content was complete. Therefore, all participants received the same training content, but susceptibility claims included prior to and after the training varied by condition. Participants were randomly assigned to conditions with a high susceptibility claim or low susceptibility claim. Following successful manipulations in prior research (e.g., Boss et al., 2015), those in the high susceptibility condition heard and were shown the following statement: "Your chances of being affected by cyber threats in the next three months are very high. So, you will need to be prepared to take action to protect yourself". Those in the low threat susceptibility condition heard and were shown the following statement "Your chances of being affected by cyber threats in the next three months are relatively low. But you will need to be prepared to take action to protect yourself". To test this manipulation, participants were asked if they were at risk from each threat in the next three months (see Appendix C). As shown in Table 1, those in the high susceptibility claim condition reported significantly greater perceived susceptibility than those in the low condition. Therefore, the threat susceptibility claim manipulation was judged to be successful. To ensure that susceptibility was not confounded with the type of threat, we also compared phishing susceptibility to password cracking susceptibility and did not observe any significant differences, t(135) = .729; p = .467. Participants reported feeling equally susceptible to phishing and password cracking attacks.

5. Experiment 2

To test H1 and H2, we conducted a field experiment. In addition to intentions captured following the training session, we also recorded precaution-taking behaviour prior to and several months after the session during two mock password-cracking attacks and three mock phishing attacks. The password and phishing attacks targeted participants' university credentials which provide access to university digital resources (e.g., network and storage access), financial and academic records, and personal data stored by the university.

5.1. Participants

A total of 2786 faculty, staff, and students were invited to the voluntary SETA initiative. Prospective participants were all members of the same university college and were incentivised to participate by repeated invitations from college leaders and by being entered in a drawing for four iPad mini 4 s. A total of 195 participants responded to the invitation and began the training. Three participants who left one or two items blank in the survey following the training were retained in the sample through the application of a mean substitution procedure. However, 54 participants did not complete the survey following the training and were excluded from further analysis. Therefore, a total of 138 participants comprised the sample (a 5.0% response rate). Of the sample, 58% were faculty and staff; the remaining 42% were students. As Table 2 illustrates, password security and protection from phishing attacks were relevant IT security threats for participants.

5.2. Training materials

Participants in the field experiment participated in the same SETA initiative as those in the pilot. Participants found the training material helpful for all topics the training covered (password management M = 4.35 SD = .82; avoiding phishing: M = 4.30, SD = .75).

5.3. Independent, dependent, and control variables

Similar to experiment 1, threat characteristics (overt [phishing] versus furtive [password cracking]) and the level of susceptibility claimed in the SETA initiative served as independent variables in experiment 2. Susceptibility claims were again manipulated with statements that participants both saw and heard regarding how likely cyber threats would be in the coming three months and participants were randomly assigned to susceptibility claim conditions.

Intentions to follow SETA guidelines regarding password maintenance and avoiding phishing attacks were gathered immediately following the training and served as one dependent variable. Intention measurement followed previous literature (e.g., Boss et al., 2015) and measurement properties of intentions to follow password and anti-phishing guidelines were satisfactory. All items are listed in Appendix C.

In addition to intentions, actual behaviour was also recorded through approximately 11 weeks and served as another dependent variable. Figure 3 shows the timeline of capturing precaution-taking behaviours.

Table 1. Results of manipulation check for threat susceptibility claim.

Threat	High Susceptibility Mean (SD)	Low Threat Susceptibility Mean (SD)	Test
Password Cracking	3.189 (.970)	2.732 (.911)	t(134) = 2.835; p = .005
Phishing	3.328 (1.120)	2.690 (.859)	t(134) = 3.746; p < .001

Table 2. Self-reported experience with IT security threats.

Item	"Yes"	"Not Sure"	"No"
Do you use your browser to store your …			
University Password	41.3%	5.1%	53.6%
Banking Password	4.3%	5.1%	90.6%
Have you ever …			
Been phished	40.6%	21.7%	37.7%
Known someone who was phished	55.1%	17.4%	27.5%
Had your identity stolen	14.5%	3.6%	81.9%

Consistent with prior phishing research (Kumaraguru et al., 2009), the IT security department notified college members of the SETA initiative and that the mock password and phishing attacks would occur. Prior to any data collection, college members were told they that they would be invited to participate in an online cyber-hygiene training and that the effectiveness of the training would be tested by a series of mock password and phishing attacks. Approximately two weeks after the initial notification,[5] the first round of mock password and phishing attacks were performed. This first round served as a baseline against which the subsequent mock password and phishing attacks were compared. Mock password attacks were performed with commercial security software called L0phtcrack.[6] Each mock password attack lasted approximately 5 days and tested whether or not passwords could be decrypted. Results included the method of decryption (e.g., brute force, dictionary, hybrid), time required to decrypt the password, password length (if applicable), and age of the password. To increase generalisability and in agreement with the IT security department, each mock phishing attack included three message types: 1) a drive-by attack during which participants were enticed to simply click on a link; 2) a form attack during which participants were lured to click on a link that led to an online form soliciting their university credentials; and 3) an attachment attack during which participants were enticed to open an attachment. Participants were randomly assigned to one of the three types of phishing messages, and the messages were randomly ordered across the three rounds.[7] A participant was successfully phished if he or she clicked on the link in a message or downloaded the attachment.

After the first round was complete, participants were invited to complete the training (which included the manipulations for susceptibility claims). The training was available for 10 days. Approximately one week after training closed, the second round of mock phishing attacks commenced. Approximately two weeks following the second mock phishing attack, the second password cracking attack was performed and one week later, the third and final round of mock phishing was conducted. All the mock attacks were performed by the university IT security department. The data were then combined, anonymised, and delivered to the authors for analysis.

To isolate the effect of threat susceptibility claims and remedy past theoretical issues, we also included several control variables in the analyses. Attitudes concerning response efficacy, threat severity, self-efficacy, the cost of following the guidelines, and the rewards of not following the guidelines were gathered following the training. Items for these variables were adapted from Boss et al. (2015) and demonstrated satisfactory measurement properties. The items and measurement properties are reported in Appendix C.

5.4. Results

Table 3 shows the means and standard deviations for intentions to follow the password maintenance and anti-phishing guidelines as well as all the control variables. To understand how susceptibility claims influenced intentions to follow the SETA guidelines, we combined responses concerning phishing and passwords into a single data file and used a General Estimating Equation (GEE, SPSS v24) for analysis. The GEE accommodates correlated responses (i.e., participant's responses about phishing and password guidelines) and the mix of binary and continuous explanatory variables. The GEE used a linear link function to model intentions and an unstructured correlation matrix to model correlated responses.[8] The results from the GEE are shown in Table 4.

Support for H1 would be evidenced by a significant threat overtness × susceptibility claim interaction that could then be interpreted. However, the analysis failed to produce a significant interaction coefficient (p = .458), therefore we halted further analysis. This finding is inconsistent with H1. Instead, self-efficacy significantly increased intention to follow the SETA guidelines for passwords and avoiding phishing.

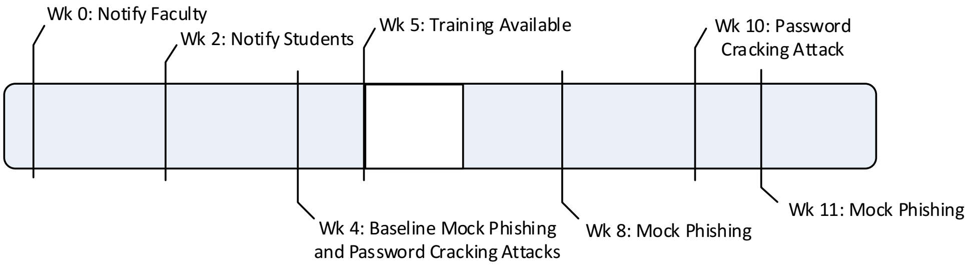

Figure 3. Timeline of field experiment.

Table 3. Means and standard deviations from experiment 2.

Measure		Password Maintenance (SD)	Avoiding phishing (SD)
Intentions to Follow Guidelines	High Susceptibility Claim	4.274 (.756)	4.479 (.598)
	Low Susceptibility Claim	4.101 (.845)	4.286 (.739)
	Total	4.188 (.803)	4.382 (.677)
Response Efficacy[a]		4.664 (.718)	4.664 (.718)
Threat Severity[a]		4.453 (.725)	4.453 (.725)
Self-Efficacy		3.837 (.921)	4.261 (.706)
Cost of Following Guidelines		2.437 (.736)	2.269 (.710)
Rewards of Not Following Guidelines		2.052 (.875)	1.887 (.848)

[a] In the field experiment, response efficacy and threat severity were measured once for both threats (see Appendix C).

Table 4. Experiment 2 results for intentions to comply with SETA guidelines.

Model Factor	B	S.E.	Wald χ^2	Df	Sig.
Intercept	−0.458	0.4645	0.973	1	0.324
Threat Overtness	0.026	0.0479	0.300	1	0.584
Susceptibility Claim	−0.074	0.0656	1.276	1	0.259
Threat × Susceptibility Claim	−0.053	0.071	0.550	1	0.458
Response Efficacy	0.020	0.0622	0.102	1	0.750
Threat Severity	0.087	0.0627	1.940	1	0.164
Self-Efficacy	0.548	0.1083	25.620	1	<0.001
Cost of Following Guidelines	−0.176	0.1381	1.627	1	0.202
Rewards of Not Following Guidelines	0.015	0.0502	0.085	1	0.770

Table 5 shows the participants' actions during rounds of mock password attacks. Table 6 shows participants' responses during the rounds of mock phishing attacks.

To understand what reduced the likelihood of a cracked password or successful phishing attack, we conducted another GEE using the combined data from the mock phishing and password attacks. The GEE used an unstructured correlation matrix and a binary logistic link function to accommodate the binary response variable (i.e., whether or not the attack was successful).

Since precaution-taking behaviour was tested in two rounds for passwords and three rounds for phishing, the results from rounds two and three of the mock phishing attacks were combined such that participants were labelled as successfully phished if they fell for the attack in either round two or three. In addition to the control variables used to predict intentions, we also included as control variables participants' performance in round one of the mock passwords and phishing attacks to clearly identify improvements over baseline in precaution-taking behaviour. We controlled for the type of phishing messages participants received by including dummy variables for drive-by and form phishing attacks. Finally, to examine the potential relationship between intentions and behaviour, we also included intentions to comply with the SETA guidelines in the analysis.

Table 5. Descriptive results of mock password-cracking attack results.

Variables	Round 1	Round 2
Average age of password (days)	1156.15	1170.68
Number of cracked passwords	48	40
Number of password changes	-	8

Table 6. Descriptive results of mock phishing attack results.

Variables	Round 1	Round 2	Round 3
Phishing responses in high susceptibility claim condition	9 (13.0%)	4 (5.8%)	5 (7.2%)
Phishing responses in low susceptibility claim condition	8 (11.6%)	11 (15.9%)	12 (17.4%)
Phishing responses to drive-by messages	4 (8.7%)	0 (0.0%)	5 (10.9%)
Phishing responses to form messages	4 (9.5%)	2 (4.8%)	3 (7.1%)
Phishing responses to attachment messages	9 (18.0%)	13 (26.0%)	9 (18.0%)
Total responses to phishing	17 (12.3%)	15 (10.9%)	17 (12.3%)

With a logistic link function, a limited response rate, and a high number of control variables modelled, our sample was less than the recommendation for power (Hosmer & Lemeshow, 2000). Following other IT security field research (e.g., Jensen et al., 2017), we retained the control variables to maintain a conservative analysis approach and rule out potential competing explanations for our findings. Additionally, fear appeal theory mandates the presence of most control variables. The results of the analysis are shown in Table 7.

The results show a significant main effect for threat overtness (p = .002) and, consistent with our arguments, an interaction between the level of contact from the threat and susceptibility claims that approaches significance (p = .092). We also note the prominent effect from round one performance (p < .001). The threat overtness × susceptibility claim interaction is illustrated in Figure 4.[9] In a logistic model, the effect of an explanatory variable depends on the values of other explanatory variables in the function (Hoetker, 2007). Therefore, we illustrate the interaction for cases when the round one attacks were successful and when they were not. Type of phishing attack also produced significant effects and response efficacy produced an effect that approached significance. Since such tests of interactions typically have low power relative to main effects (Brookes et al., 2004), we performed additional analysis to interpret the effects of threat overtness and susceptibility claims.

Table 7. Experiment 2 results for precaution-taking behaviour.

Model Factor	B	S.E.	Wald χ^2	Df	Sig.
Intercept	−3.445	1.0062	11.722	1	0.001
Threat Overtness	1.67	0.5332	9.813	1	0.002
Susceptibility Claim	−0.123	0.4204	0.085	1	0.771
Threat × Susceptibility Claim	1.384	0.8213	2.84	1	0.092
Response Efficacy	−0.414	0.2465	2.822	1	0.093
Threat Severity	0.143	0.2154	0.442	1	0.506
Self-Efficacy	0.240	0.3101	0.599	1	0.439
Cost of Following Guidelines	0.127	0.5724	0.049	1	0.825
Rewards of Not Following Guidelines	−0.210	0.2474	0.724	1	0.395
Round 1 Performance (Clicked or Cracked)	2.935	0.3736	61.71	1	<0.001
Drive By Attack	−1.600	0.7486	4.57	1	0.033
Form Attack	−1.633	0.8561	3.638	1	0.056
Intent	0.100	0.3243	0.094	1	0.759

Following Boss et al. (2015), we split the analysis by condition to examine the effect of susceptibility claims for each threat separately. We performed two additional GEEs: one for password maintenance (furtive) and one for phishing (overt). Both GEEs used unstructured correlation matrices and a binary logistic link function. The results are shown in Table 8.

When the main and interaction effects for susceptibility claims are dissected, a significant effect for susceptibility claims emerges for avoiding phishing (p = .026). But no effect from susceptibility claims is observed for password maintenance (p = .475). This pattern of findings is consistent with H2. Round one performance remains significant for both avoiding phishing and password maintenance and type of phishing attack remains significant for avoiding phishing. Additionally, intent to comply with password guidelines approaches significance. However, the direction of the coefficients for self-efficacy is inconsistent. On one hand, higher self-efficacy reduces the likelihood of being phished. But, on the other hand, higher self-efficacy increases the likelihood of a cracked password. Additional analysis concerning the effect of susceptibility claims on the length of time required for a password crack is in Appendix D.

6. Discussion

The paper focuses on how threat characteristics (overt versus furtive attacks) shape individuals' attitudes regarding threats and how these attitudes subsequently anchor individuals' responses to new claims about the threats. Our results add nuance to contradictory findings regarding threat susceptibility, intentions for precaution-taking behaviour, and the performance of actual behaviour. To explore contradictory findings that occur in the extant literature, we introduced SJT. SJT postulates that when individuals receive persuasive messages, they compare the message claims against anchors of their existing attitudes. Persuasive claims that are too far from existing attitudes will be ignored, while claims that closely approximate existing attitudes will be assimilated. Claims most likely to persuade will be far enough from anchors to justify behaviour change, but not far enough to be rejected as unreasonable.

Contrary to our expectations (H1), susceptibility claims played no detectable role in predicting intentions to follow the SETA guidelines. Rather, self-efficacy proved more influential on intentions to comply with the guidelines. These results corroborate the argument that for predicting intentions, susceptibility claims will likely have a modest effect. However, when behaviour is examined, a different story regarding threat susceptibility emerged. When susceptibility claims were used to motivate precaution-taking against a furtive attack, they again failed to motivate behaviour change. But, when susceptibility claims were used to motivate precaution-taking against overt attacks, their effect on behaviour was significant (H2). The implications of these findings are elaborated below.

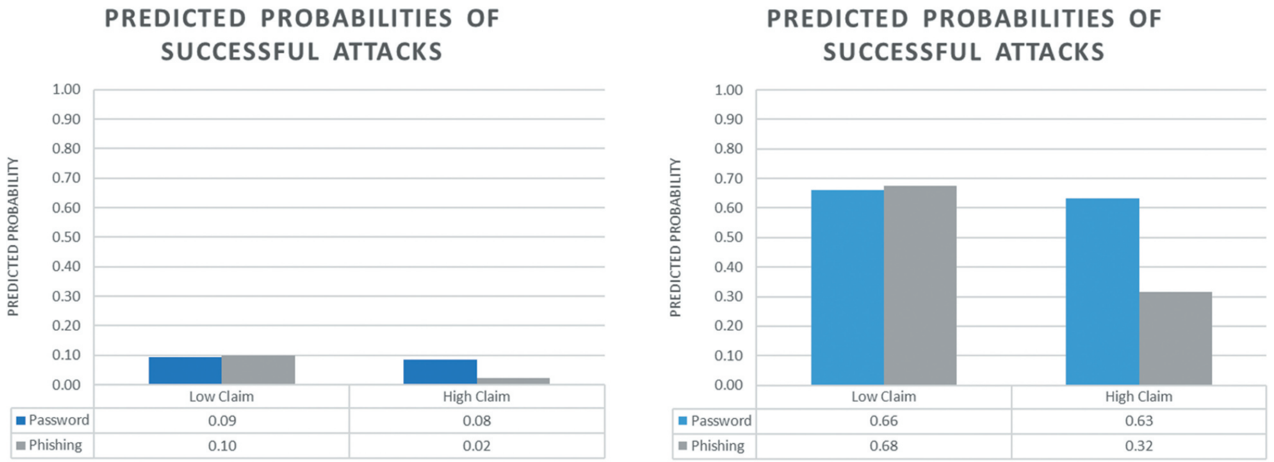

Figure 4. Illustration of the Threat × Susceptibility Claim interaction when round one attacks were unsuccessful (left) and successful (right).

Table 8. Experiment 2 results of password maintenance and avoiding phishing.

Model Factor	B	S.E.	Wald χ^2	Df	Sig.
Password Maintenance					
Intercept	0.771	2.2276	0.120	1	0.729
Susceptibility Claim	−0.477	0.6676	0.511	1	0.475
Response Efficacy	−0.814	0.5086	2.562	1	0.109
Threat Severity	0.408	0.3447	1.400	1	0.237
Self-Efficacy	1.750	0.7163	5.966	1	0.015
Cost of Following Guidelines	1.530	1.0153	2.270	1	0.132
Rewards of Not Following Guidelines	−0.362	0.491	0.543	1	0.461
Round 1 Performance (Clicked or Cracked)	4.823	0.8689	30.814	1	<0.001
Intent	−0.962	0.525	3.357	1	0.067
Avoiding Phishing					
Intercept	3.889	2.020	3.706	1	0.054
Susceptibility Claim	−1.120	0.502	4.981	1	0.026
Response Efficacy	−0.134	0.283	0.223	1	0.637
Threat Severity	0.030	0.3194	0.009	1	0.926
Self-Efficacy	−1.169	0.6156	3.604	1	0.058
Cost of Following Guidelines	−0.546	0.763	0.512	1	0.474
Rewards of Not Following Guidelines	−0.208	0.441	0.222	1	0.637
Round 1 Performance (Clicked or Cracked)	1.278	0.5974	4.580	1	0.032
Drive By Attack[a]	−1.487	0.6192	5.764	1	0.016
Form Attack[a]	−1.696	0.6316	7.211	1	0.007
Intent	1.069	0.6501	2.705	1	0.100

[a] Applicable only for phishing attacks.

6.1. Implications for theory

First, we present clear evidence of the variable effect of SETA initiatives using susceptibility claims to motivate compliance. In an extension to past IT security theorising, our findings suggest that overtness of the threat influences whether individuals will respond to interventions designed to increase precaution-taking behaviour. If individuals are directly targeted by overt threats, interventions invoking susceptibility claims will be more effective because the claims will fall in latitudes of the belief that individuals find acceptable. If susceptibility claims in SETA campaigns are too far from existing attitudes, the claims will be unlikely to produce behaviour change. This pattern of results is consistent with SJT's core prediction in, what is to our knowledge, the theory's first test in IS security. This conclusion also corroborates observations made by others (e.g., Karjalainen & Siponen, 2011) who claimed that training in SETA campaigns should build on participants' collective experiences and understanding of attacks. Additional research is required to understand how latitudes of acceptance, non-commitment, and rejection may change as people mature in their attitudes about threats. However, an important implication of this research is that furtive attacks likely contribute to anchors that are associated with wider latitudes of rejection.

Second, the categorisation of IT security threats by overtness provides a theoretically meaningful and useful way to segregate IT security threats and examine their disparate effects. As IT departments grapple to educate organisation members about security, understanding how threat characteristics hamper or enhance precaution taking is likely to become increasingly important. Our findings have shown that threat characteristics and the attitudes that individuals form in response significantly affect what interventions will be successful in mitigating the threat. Future scholars and practitioners will need to be aware of how threat characteristics can shape individuals' attitudes. Overtness of IT security threats may be one characteristic of a taxonomy of IT security threats that could govern how individuals will respond to training interventions. We invite others to contribute to this under-theorised, yet critical area of IT security research.

Third, our findings also offer evidence that the effect from latitudes of belief operates independently from self-reported perceptions of susceptibility. In experiment 1, participants reported that they felt more susceptible to both phishing and password-cracking attacks after being exposed to high susceptibility claims in the training. However, this increase in susceptibility perceptions did not translate to an increase in intentions to comply with the SETA guidelines and did not increase precaution-taking behaviour against password cracking in the field experiment. Moreover, we observed a reversal in the effect of self-efficacy on precaution-taking behaviour. It is possible that claims in SETA initiatives about other fear appeal variables may be placed in latitudes of acceptance, non-commitment, and rejection and that claims that are too distant from anchors of prior attitudes will be ignored in a fashion similar to susceptibility claims.

Fourth, the unique design of this study, which incorporated a test of precaution-taking behaviour prior to any intervention, allowed observation of a critical contributor to IT security vulnerability. Out of all variables predicting password cracking or phishing success, the most influential was whether a person was successfully attacked in the first round. Given the small number of people who updated their passwords in response to training, this was not surprising for the password-cracking attack. But the prior performance was also a significant predictor for subsequent phishing success. This finding underscores the durability of anchors from existing attitudes and suggests that some individuals are consistently more vulnerable to password and phishing attacks than others. Additional study of these individuals' latitudes of beliefs could reveal explanations for the individuals' resistance to training. Additional extensions based on this finding could include isolating characteristics that identify these individuals and creating SETA initiatives and other interventions (e.g., limiting of access) that effectively reduce the risk they introduce.

Finally, our results echo the findings from other scholars (e.g., Crossler et al., 2014; Vance et al., 2014) who discovered a discrepancy between what individuals report they intend to do and what they actually do. We noted participants in both experiments reported very strong intentions to follow the SETA guidelines (Password maintenance: M = 4.19, SD = .80; Phishing avoidance: M = 4.38, SD = 4.38). Yet, the relationship between intent and successful attack was marginally significant for passwords and not significant for phishing. Although our analysis was underpowered, this finding emphasises the need to investigate intentions alongside precaution-taking behaviour in naturalistic settings. Such investigations are critical to advance the field of IT security research.

6.2. Implications for practice

Our results have several implications for practice. Foremost is to carefully consider potential anchors from existing attitudes that may distort claims made in SETA campaigns. Campaigns containing claims about threats that come into direct contact with employees are likely to be more successful because the claims will be near employees' anchors of existing attitudes. These claims will likely be interpreted as credible and will be more likely to bring about desired behaviour change. Claims falling in the latitude of rejection will likely yield feelings of irrelevance, derogation of training, and ultimately little behaviour change. This finding could assist organisation leaders as they decide how to invest their IT training budgets. For example, organisation leaders may be more successful with SETA initiatives when threats they are trying to counter are overt (see Table A1 for potential overt threats). But the finding also raises the question of what to do when organisations must enlist the efforts of their members in defence against an organisational threat which is transparent to individuals. Prior research (e.g., Johnston et al., 2015; Willison, Lowry et al., 2018) has suggested sanctions or deterrence may offer potential remedies. Another option could be mandated that limit risk exposure for furtive type attacks. For example, many organisations have password requirements and expiration policies that are electronically enforced. Our research implies that making the threat less transparent and more directly experienced could be another avenue to motivate users to comply with SETA guidelines. For example, the IT security department might notify organisational users when they have detected several failed login attempts. Such notifications would make furtive attacks more overt and could alter anchors of existing attitudes. Another approach may be to use SETA initiatives that create realistic experiences with threats. Making threats more noticeable may run counter to prevailing practices in many IT security departments. But it may contribute to an environment in which users are eager to change their behaviour to escape the threats they face.

Finally, organisations face significant challenges when dealing with individuals who are targets of repeated successful attacks. It is clear that such individuals need additional attention, but less clear is what methods will more effectively sensitise these individuals to IT security threats. Future research should consider the effect of screening, specialised training, curtailing of privileges, sanctions, and other interventions on this narrow group. Any gains with this vulnerable group are likely to lead to disproportionate gains in overall IT security.

7. Limitations and future steps

There are several limitations of this research, which should be considered along with our conclusions. First, we acknowledge that the number of observations in the field experiment is a limitation. As a result, we adopted a conservative stance in interpreting the findings and still uncovered significant findings despite the lack of power. A larger sample may have resulted in other factors being statistically significant in our model, though it is unlikely that the variables that are currently significant would change (Cohen, 1992). Nevertheless, our sample size may have occluded other significant relationships. Further, participants could have responded to phishing attacks by mistake. However, we randomly assigned participants to experimental conditions, so we expect the effect from this issue to be minor. Next, our data collection took place in an academic setting. Although universities have had significant loses and are common targets of cybercriminals, we acknowledge that organisational expectations, practices, and constraints of the academic environment may differ from those of other organisations. Therefore, we recommend replication with different samples, in different organisations. Finally, there are several important extensions of this work. In particular, we note the testing of interactions between the claimed and experienced levels of other fear appeal variables, testing of other threats, and development of interventions intended for particularly vulnerable individuals.

8. Conclusion

Organisations face significant risks from rising IT security threats. In this longitudinal field experiment, we examined the factors that influence change in security behaviour. Specifically, we were interested in understanding what motivates users to protect themselves from some of the most prevalent cyber attacks: attacks on passwords and phishing attacks via email. Utilising social judgement theory, we found that threat characteristics and individuals' corresponding attitudes impacted how individuals responded to susceptibility claims in training about the threat. By attending to this finding, organisation leaders and can increase the effectiveness of their SETA initiatives. These results shed light on empirical inconsistencies and deepen theorising about fear appeals used to motivate precaution-taking behaviour.

Notes

1. Many other theories focus on the effect of *external* reference points that individuals may use to evaluate a persuasive message. For example, dual process theory addresses peripheral or heuristic-supporting message cues, credibility of the message sender, or order of messages (Ho & Bodoff, 2014; Meservy et al., 2014). SJT's focus on prior attitudes as a powerful *internal*

reference point is unique among of theories of persuasion (Eagly & Chaiken, 1993).

2. Substantial previous work within and outside the information systems discipline has posited a positive relationship between intentions and behaviour. Although we empirically examine this relationship, we do not offer additional theorising beyond what has previously been argued and therefore we do not explicitly hypothesise this relationship.
3. Participants were asked "The ____ section was helpful" and the items were rated on a 5-point scale with Strongly Disagree and Strongly Agree as the endpoints.
4. The item used to measure perceived frequency is "Please indicate the frequency you experience attacks against your IT security" measured on a 5-point scale with "Never" and "Always" as endpoints.
5. Faculty and students were notified of the project at different times. Students were notified later and the notification took place approximately 2 weeks prior to the round one attacks (see Figure 2).
6. L0phtcrack (http://www.l0phtcrack.com/) takes as input the encrypted list of user credentials and through brute force, dictionaries, and rainbow tables attempts to crack the encryption.
7. Once participants were randomly assigned to a type of phishing attack, they only received that type of attack. The type of phishing attack and the round is also included in the analysis. See Tables 7 and 8.
8. AR(1), exchangeable, M-dependent, and unstructured correlation structures were all tested to determine which structure was most suitable in the analysis. No differences were observed between the correlation structures for the analysis for intentions or the analysis for behaviour.
9. To calculate predicted probabilities, mean values for response efficacy, threat severity, self-efficacy, cost of following guidelines, and rewards of not following guidelines were used for each threat. Additionally, drive-by phishing attacks were compared to password cracking attacks.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This research was supported by a grant from the U.S. National Science Foundation (NSF) Social and Economic Division, Project# 1421580. The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied, of NSF or the U.S. Government.

ORCID

Matthew L. Jensen http://orcid.org/0000-0001-8711-1827
Alexandra Durcikova http://orcid.org/0000-0002-6705-202X
Ryan T Wright http://orcid.org/0000-0002-9719-415X

References

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. *Economics of Information Security*, *12*(1), 165–178. https://doi.org/10.1007/1-4020-8090-5_13

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Anti-Phishing Working Group. (2016). *Phishing activity trends report*. Retrieved July 15, 2016, from https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

Ashford, W. (2018). *Nearly half of UK manufacturers hit by cyber attacks*. Computer Weekly. Retrieved May 14, 2018, from https://www.computerweekly.com/news/252439718/Nearly-half-of-UK-manufacturers-hit-by-cyber-attacks

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. https://doi.org/10.17705/1jais.00506

Barrett, B. (2016). *Some basic security tips for the clinton campaign (and anyone else)*. Wired Magazine. Retrieved October 14, 2016, from https://www.wired.com/2016/10/basic-security-tips-clinton-campaign-anyone-else/

Basu, E. (2014). *Target CEO fired –Can you be fired if your company is hacked?* Forbes Magazine. https://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-fired-can-you-be-fired-if-your-company-is-hacked/#57e47c987c9f

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Brookes, S. T., Whitely, E., Egger, M., Smith, G. D., Mulheran, P. A., & Peters, T. J. (2004). Subgroup analyses in randomized trials: Risks of subgroup-specific analyses;: Power and sample size for the interaction test. *Journal of Clinical Epidemiology*, *57*(3), 229–236. https://doi.org/10.1016/j.jclinepi.2003.08.009

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Carvalho, S. W., Block, L. G., Sivaramakrishnan, S., Manchanda, R. V., & Mitakakis, C. (2008). Risk perception and risk avoidance: The role of cultural identity and personal relevance. *International Journal of Research in Marketing*, *25*(4), 319–326. https://doi.org/10.1016/j.ijresmar.2008.06.005

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205–222. https://doi.org/10.25300/MISQ/2016/40.1.09

Cohen, J. (1992). Statistical power analysis. *Current Directions in Psychological Science*, *1*(3), 98–101. https://doi.org/10.1111/1467-8721.ep10768783

Corfield, G. (2019). *Personal data slurped in Airbus hack – But firm's industrial smarts could be what crooks are after*. The Register. Retrieved April 15, 2019, from https://www.theregister.co.uk/2019/01/31/airbus_hacked_eurofighter_link/

Crossler, R. E. (2010). *Protection motivation theory: Understanding determinants to backing up personal data. Paper presented at the 43rd Hawaii International Conference on System Sciences (HICSS)*. Hawaii.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226. https://doi.org/10.2308/isys-50704

De Castella, K., McGarty, C., & Musgrove, L. (2009). Fear appeals in political rhetoric about terrorism: An analysis of speeches by Australian Prime Minister Howard. *Political Psychology*, *30*(1), 1–26. https://doi.org/10.1111/j.1467-9221.2008.00678.x

De Guinea, A. O., & Markus, M. L. (2009). Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *MIS Quarterly*, *33*(3), 433–444. https://doi.org/10.2307/20650303

Disparte, D., & Furlow, C. (2017). The best cybersecurity investment you can make is better training. *Harvard Business Review*, *5*. https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

DUO. (2016). *Inside a retail hack: Lateral movement & credential-harvesting*. DUO Inc. Retrieved October 14, 2016, from https://duo.com/blog/inside-a-retail-hack-lateral-movement-and-credential-harvesting

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers.

Easterling, D. V., & Leventhal, H. (1989). Contribution of concrete cognition to emotion: Neutral symptoms as elicitors of worry about cancer. *Journal of Applied Psychology*, *74*(5), 787–796. https://doi.org/10.1037/0021-9010.74.5.787

Etters, K. (2019). *Cyberattack diverts almost $500,000 out of city of Tallahassee payroll account*. USA Today. Retrieved April 15, 2019, from https://www.usatoday.com/story/news/nation/2019/04/05/hackers-divert-nearly-500-000-city-tallahassees-payroll/3383451002/

FBI. (2016). *FBI warns of dramatic increase in business E-Mail scams*. Federal Bureau of Investigation. Retrieved June 14, 2016, from https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

Fitzgerald, D. (2016). *Akamai says hackers use 'smart' devices to test stolen usernames, passwords*. Wall Street Journal. Retrieved October 14, 2016, from http://www.wsj.com/articles/akamai-says-hackers-use-smart-devices-to-test-stolen-usernames-passwords-1476287922

Gartner. (2018). *Gartner forecasts worldwide information security spending to exceed $124 billion in 2019*. Gartner Inc. Retrieved April 14, 2019, from https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Givens, S. (2019). *Five strategies to get employee buy-in for security awareness training*. Forbes Magazine. Retrieved April 13, 2019, from https://www.forbes.com/sites/forbeshumanresourcescouncil/2019/04/12/five-strategies-to-get-employee-buy-in-for-security-awareness-training/#1e6262fc236d

Grover, V., Lyytinen, K., Srinivasan, A., & Tan, B. C. Y. (2008). Contributing to rigorous and forward thinking explanatory theory. *Journal of the Association for Information Systems*, *9*(2), 40–47. https://doi.org/10.17705/1jais.00151

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

Ho, S. Y., & Bodoff, D. (2014). The effects of web personalization on user attitude and behavior: An integration of the elaboration likelihood model and consumer search theory. *MIS Quarterly*, *38*(2), 497–520. https://doi.org/10.25300/MISQ/2014/38.2.08

Hoetker, G. (2007). The use of logit and probit models in strategic management research: Critical issues. *Strategic Management Journal*, *28*(4), 331–343. https://doi.org/10.1002/smj.582

Hosmer, D. W., & Lemeshow, S. (2000). *Applied logistic regression*. Wiley.

Huigang, L., & Yajiong, X. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75–78. https://doi.org/10.1145/975817.975820

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*(2), 245–284. https://doi.org/10.1111/deci.12328

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

Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06

Kankanhalli, A., Teo, -H.-H., Tan, B. C. Y., & Wei, -K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kaplan, E. L., & Meier, P. (1958). Nonparametric estimation from incomplete observations. *Journal of the American Statistical Association*, *53*(282), 457–481. https://doi.org/10.1080/01621459.1958.10501452

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518. https://doi.org/10.17705/1jais.00274

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). *School of phish: A real-world evaluation of anti-phishing training. Paper presented at the SOUPS '09 proceedings of the 5th symposium on usable privacy and security*, Mountain View, CA.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching johnny not to fall for phish.

ACM Transactions on Internet Technology (TOIT), *10*(2), 7. https://doi.org/10.1145/1754393.1754396

LaTour, M. S., & Pitts, R. E. (1989). Using fear appeals in advertising for aids prevention in the college age population. *Marketing Health Services*, *9*(3), 5–14. https://doi.org/10.1007/978-3-319-17055-8_5

Lewis, I., Watson, B., Tay, R., & White, K. M. (2007). The role of fear appeals in improving driver safety: A review of the effectiveness of fear-arousing (threat) appeals in road safety advertising. *International Journal of Behavioral Consultation and Therapy*, *3*(2), 203–222. https://doi.org/10.1037/h0100799

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, *31*(4), 705–737. https://doi.org/10.2307/25148817

Mantel, N. (1966). Evaluation of survival data and two new rank order statistics arising in its consideration. *Cancer Chemotherapy Reports. Part 1*, *50*(3), 163–170. https://pubmed.ncbi.nlm.nih.gov/5910392/

Martin, A. (2019). *Cybercriminals target the UK police force with ransomware*. The Inquirer. Retrieved April 15, 2019, from https://www.theinquirer.net/inquirer/news/3073016/police-federation-ransomware-attack

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Meservy, T. O., Jensen, M. L., & Fadel, K. (2014). Evaluation of competing candidate solutions in electronic networks of practice. *Information Systems Research*, *25*(1), 15–34. https://doi.org/10.1287/isre.2013.0502

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–A222. https://doi.org/10.25300/MISQ/2018/13853

National Institute of Standards and Technology. (2016). Digital authentication guidelines: National institute of standards and technology.

Oswick, C., Fleming, P., & Hanlon, G. (2011). From borrowing to blending: Rethinking the processes of organizational theory building. *Academy of Management Review*, *36*(2), 318–337. https://www.jstor.org/stable/41318003

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance. Paper presented at the 40th Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2007.206

Palfy, S. (2019). *Why reused passwords could put your tax information at risk*. Forbes Magazine. Retrieved April 22, 2019, from https://www.forbes.com/sites/forbestechcouncil/2019/04/12/why-reused-passwords-could-put-your-tax-information-at-risk/#100e3c6441f5

Pattabiraman, A., Srinivasan, S., Swaminathan, K., & Gupta, M. (2018). Fortifying corporate human wall: A literature review of security awareness and training. *Information Technology Risk Management and Compliance in Modern Organizations* (pp. 142–175): IGI Global.

Peterson, P. D., & Koulack, D. (1969). Attitude change as a function of latitudes of acceptance and rejection. *Journal of Personality and Social Psychology*, *11*(4), 309–311. https://doi.org/10.1037/h0027342

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

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

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

Reyna, V. F., & Farley, F. (2006). Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy. *Psychological Science in the Public Interest*, *7*(1), 1–44. https://doi.org/10.1111/j.1529-1006.2006.00026.x

Rhine, R. J., & Severance, L. J. (1970). Ego-involvement, discrepancy, source credibility, and attitude change. *Journal of Personality and Social Psychology*, *16*(2), 175–190. https://doi.org/10.1037/h0029832

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology:: Interdisciplinary and Applied*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A source book* (pp. 153–176). Guilford Press.

Savage, M. (2019). *Cybercrime for dummies: Cracking internet passwords is as easy as 123456*. The Guardian. Retrieved April 22, 2019, from https://www.theguardian.com/technology/2019/apr/21/cybercrime-hacking-internet-account-passwords

Shah, D. V., Faber, R. J., & Youn, S. (1999). Susceptibility and severity: Perceptual dimensions underlying the third-person effect. *Communication Research*, *26*(2), 240–267. https://doi.org/10.1177/009365099026002006

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1–36. https://doi.org/10.1080/14792772143000003

Sherif, C. W., Sherif, M., & Nebercall, R. E. (1965). *Attitude and attitude change: The social judgment-involvement approach*. Saunders.

Sherif, M., & Hovland, C. I. (1961). *Social judgment: Assimilation and contrast effects in communication and attitude change*. Yale Univer. Press.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Slater, M. D. (2006). Specification and misspecification of theoretical foundations and logic models for health communication campaigns. *Health Communication*, *20*(2), 149–157. https://doi.org/10.1207/s15327027hc2002_6

Smith, K. H., & Stutts, M. A. (2003). Effects of short-term cosmetic versus long-term health fear appeals in anti-smoking advertisements on the smoking behaviour of adolescents. *Journal of Consumer Behaviour*, *3*(2), 157–177. https://doi.org/10.1002/cb.130

Smith, S. W., Atkin, C. K., Martell, D., Allen, R., & Hembroff, L. (2006). A social judgment theory approach to conducting formative research in a social norms campaign. *Communication Theory*, *16*(1), 141–152. https://doi.org/10.1111/j.1468-2885.2006.00009.x

Solman, P. (2015). The battle to beat password security threats. *Financial Times*.

Steinberg, J. (2016). *The biggest lessons from the yahoo data breach are the ones nobody is talking about*. Inc Magazine. Retrieved October 14, 2016, from http://www.inc.com/

joseph-steinberg/the-biggest-lessons-from-the-yahoo-data-breach-are-the-ones-nobody-is-talking-ab.html

Tanner, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *The Journal of Marketing*, *55*(3), 36–45. https://doi.org/10.1177/002224299105500304

Taylor, P. J., Russ-Eft, D. F., & Chan, D. W. L. (2005). A meta-analytic review of behavior modeling training. *Journal of Applied Psychology*, *90*(4), 692–709. https://doi.org/10.1037/0021-9010.90.4.692

Teigen, K. H. (2005). The proximity heuristic in judgments of accident probabilities. *British Journal of Psychology*, *96* (4), 423–440. https://doi.org/10.1348/000712605X47431

Truex, D., Holmström, J., & Keil, M. (2006). Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems*, *7* (12), 797–821. https://doi.org/10.17705/1jais.00109

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), 679. https://doi.org/10.17705/1jais.00375

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345–366. https://doi.org/10.25300/MISQ/2015/39.2.04

Velicer, W. F., & Prochaska, J. O. (2008). Stage and non-stage theories of behavior and behavior change: A comment on schwarzer. *Applied Psychology*, *57*(1), 75–83. https://doi.org/10.1111/j.1464-0597.2007.00327.x

Verizon. (2017). *2017 Data breach investigations report*. Verizon. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the AIS*, *41*, 13. https://www.doi.org/10.17705/1CAIS.04113

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194. https://doi.org/10.17705/1jais.00424

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association for Information Systems*, *19*(12), 1187–1216. https://doi.org/10.17705/1jais.00524

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266–293. https://doi.org/10.1111/isj.12129

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

Wright, R. T., Jensen, M. L., Thatcher, J., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*(2), 385–400. https://doi.org/10.1287/isre.2014.0522

Zahedi, F. M., Abbasi, A., & Yan, C. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448–484. https://doi.org/10.17705/1jais.00399

Appendix A: effect of susceptibility

To understand the nature of the relationship between susceptibility, intentions, and behaviour that has been uncovered in the past research, we performed a systematic review of articles published in the *European Journal of Information Systems, MIS Quarterly, Information Systems Research, Journal of MIS, Information Systems Journal, Journal of Information Technology, Journal of Strategic Information Systems*, and *Journal of the AIS*. We used the following keywords in the search: SETA, security education training awareness, protection motivation theory, fear appeal, security, vulnerability, and susceptibility. This search resulted in a total of 537 articles (EJIS: 11, MISQ: 86, ISR: 57, JMIS: 105, ISJ: 24, JIT: 1, JSIS: 206, JAIS: 44). Titles and abstracts of returned articles were then manually reviewed and articles examining the effect of susceptibility were summarised in Table A1.

Appendix B: training materials

Specific instruction on password maintenance

1. When creating a good and secure password, longer is better. At a minimum, passwords must be at least 8 characters long, but 12 or even 15 characters are better.
2. It is much easier if you use a passphrase instead of a single password.
3. You can make the passphrase more difficult to crack by adding upper and lower case letters, numbers, and special characters in a way that is easy to remember.
4. Always choose a unique password for every sensitive account, for example, financial or work accounts.
5. Change your password to sensitive accounts to ensure that no one is accessing your account without your knowledge.
6. If your [University] password doesn't meet these guidelines or you haven't changed your password in the last year, you should change your password.
7. If you feel that your [University] password has been compromised, change your password immediately. [Instructions for changing password]

Specific instructions on protecting against phishing attacks

1. Never respond to a message with private information.
2. Never open an attachment or click on a link in a message from someone you don't know.
3. Hover your mouse over any embedded links in a message to make sure they are what you expect.
4. If you get a message that requests an action such as opening a file, clicking on a link, remember: Stop! Think . . ., Act. Stop!: Pause to consider the new message. Don't automatically respond as soon as a new message comes. Think . . .: Does the request concern private information? Does the request seem reasonable? Why would the sender need me to respond? Act: If anything seems suspicious, verify the message with a trusted colleague and [report the message to IT security] for additional scrutiny.
5. If you responded to a phishing message don't panic, this could happen to anyone. [Report the message to IT security]. Run a virus scan on your device. Change any affected passwords. Finally, contact [the IT security department] to get additional help to make sure your device is unaffected.

Table A1. Summary of research on the effect of susceptibility in SETA initiatives.

Study	Threat	Level of Overtness	Susceptibility → Intentions	Susceptibility → Behaviour
Anderson and Agarwal (2010)	Theft of private information on home computer	Low	Security Concern → (+) Attitude towards security related behaviour → (+) Intention to perform security-related behaviour	-
Bulgurcu et al. (2010)	Non-Compliance with information security policy	Unknown	Susceptibility → (+) Costs of non-compliance → (+) Attitude → (+) Intention	-
Huigang and Yajiong (2010)	Spyware	Low	Susceptibility → (+) Perceived threat → (+) Avoidance Motivation (Intention)	Susceptibility → (+) Perceived threat → (+) Avoidance motivation (intention) → (+) Avoidance behaviour (self-reported)
Johnston and Warkentin (2010)	Spyware	Low	N.S.	-
Vance et al. (2014)	Malware	Moderate	-	N.S.
Boss et al. (2015)	Data loss; Malware	High-Moderate	Data loss: High fear susceptibility → (+) Intention; Malware: High fear susceptibility → (+) Intention	Data loss and Malware: Intention → (+) Behaviour
Johnston et al. (2015)	Password theft; Unencrypted USB devices; Failure to logout of workstations	High-Moderate	N.S.	-
Posey et al. (2015)	Non-Compliance with information security policy (various)	Unknown	Not assessed due to measurement issues	Not assessed due to measurement issues
Zahedi et al. (2015)	Malicious websites	Moderate	N.S.	-
Chen and Zahedi (2016)	Internet attacks (various)	High-Moderate	-	Susceptibility → (+) Perceived threat → (+) Protective actions (self-reported) and (+) Seeking help (self-reported) and (+) Avoidance (self-reported)
Warkentin et al. (2016)	Theft; negligence; Website defacement; Malware; Overheating; Natural disasters	High-Low	-	Threat appraisal → (+) Self-referential thinking
Johnston et al. (2016)	Ignoring password encryption	Low	Direct model: Susceptibility → (+) Intention to Violate Policy Moderated model: N.S.	-
Menard et al. (2017)	Password theft	Low	N.S.	-
Moody et al. (2018)	Password sharing; USB practices; Locking computers	High-Moderate	Perceived threat → (+) Fear	-

Appendix C: measurement

Threat susceptibility should be considered in the context of fear appeal theory because it is one factor describing a threat that should motivate behaviour change as individuals attempt to escape the threat. Therefore, we captured and included in the analysis all of the core constructs of fear appeal theory (e.g., susceptibility, threat severity, response efficacy, self-efficacy), several constructs that have been added through subsequent research (e.g., costs of following guidelines and rewards of not following guidelines), and factors that were unique to our data collection (e.g., type of phishing attacks). In addition to threat susceptibility, threat severity and response efficacy were originally intended to serve as manipulated variables in experiment 2, and participants were randomly assigned to high and low conditions of each treatment (see Table C1). Participants were shown and heard statements relevant to their condition in the introduction and conclusion of the training.

The manipulations for these variables were tested immediately following the training session with the following items and responses on a 1–5 (Strongly disagree – Strongly agree) scale. Threat severity: "Cyber threats can have severe consequences for me". Response efficacy: "The actions suggested by the training will provide me with effective protection against cyber threats". Threat susceptibility: "I am vulnerable to cyber threats".

After data collection was complete, we determined that the number of participants who completed the training did not support the inclusion of threat severity and response efficacy. Additionally, the manipulation checks for these variables failed (Threat severity: t(136) =.039, p =.969 and Response efficacy: t(136) =.459, p =.774). As a result, these variables were not included as manipulations in experiment 2. However, as argued above, susceptibility claims should be examined in the context of fear appeal theory and threat severity and response efficacy constitute important factors in fear appeal theory. Therefore, the manipulation check items for threat severity and response efficacy were included in the analysis as control variables.

Consistent with experiment 1, only threat susceptibility produced a perceivable difference in experiment 2. But the effect only approached significance: Threat susceptibility: t (136) = 1.615, p =.109; M_{high} = 4.25, SD_{high} =.96; M_{low} = 3.97, SD_{low} = 1.03. Since the manipulation check was successful in experiment 1 and the effect for susceptibility claims was significant in experiment 2, we reported the results but note this finding as an important limitation. Measurement properties of the remaining factors (rewards of non-compliance, costs of compliance, self-efficacy, and intentions) are shown in Tables C2 and C3.

Table C1. Original manipulations for experiment 2.

Condition	Text of Manipulation
High Threat Severity Claims	Cyber threats have serious consequences (e.g., loss of financial or private information) for organisations and individuals.
Low Threat Severity Claims	Cyber threats are a source of annoyance for organisations and individuals.
High Response Efficacy Claims	Following the guidelines in this training will provide effective protection against common cyber threats.
Low Response Efficacy Claims	Following the guidelines in this training will provide some protection against common cyber threats.
High Threat Susceptibility Claims	Your chances of being affected by cyber threats in the next three months are very high. So, you will need to be prepared to take action to protect yourself
Low Threat Susceptibility Claims	Your chances of being affected by cyber threats in the next three months are relatively low. But you will need to be prepared to take action to protect yourself.

Table C2. Survey items for experiment covariates (Password | Phishing).

<table>
<tr><th>Item No.</th><th>Item Text</th><th>Item Loading</th><th>CR</th><th>AVE</th><th>α</th></tr>
<tr><td colspan="6"><b>Rewards</b> (Boss et al., 2015)</td></tr>
<tr><td>RWD1</td><td>Not following guidelines for (passwords/phishing) saves me time. [Reverse coded]</td><td>0.875 | 0.529</td><td>0.809 | 0.862</td><td>0.535 | 0.628</td><td>0.797 | 0.861</td></tr>
<tr><td>RWDD2</td><td>Following the guidelines in this training for (passwords/phishing) would slow me down.</td><td>0.937 | 0.578</td><td></td><td></td><td></td></tr>
<tr><td>RWD3</td><td>Following the guidelines in this training for (passwords/phishing) would slow down my computer.</td><td>0.507|0.968</td><td></td><td></td><td></td></tr>
<tr><td>RWD4</td><td>Following the guidelines in this training for (passwords/phishing) would limit the functionality of my computer.</td><td>0.491 |0.980</td><td></td><td></td><td></td></tr>
<tr><td colspan="6"><b>Cost</b> (Boss et al., 2015)</td></tr>
<tr><td>COST1</td><td>The benefits of following the guidelines for (passwords/phishing) outweigh the cost.</td><td>0.509 |0.569</td><td>0.743 | 0.819</td><td>0.512 | 0.610</td><td>0.702 | 0.809</td></tr>
<tr><td>COST2</td><td>I am discouraged to follow the guidelines for (passwords/phishing) because it would take too much time.</td><td>0.972 |0.868</td><td></td><td></td><td></td></tr>
<tr><td>COST3</td><td>I am discouraged to follow the guidelines for (passwords/phishing) because I feel silly doing so.</td><td>0.576 |0.867</td><td></td><td></td><td></td></tr>
<tr><td colspan="6"><b>Self-Efficacy</b> (Johnston et al., 2015)</td></tr>
<tr><td>SE1</td><td>It is easy to follow the guidelines for (passwords/phishing).</td><td>0.773 |0.841</td><td>0.923 | 0.927</td><td>0.752 | 0.761</td><td>0.919 | 0.929</td></tr>
<tr><td>SE2</td><td>It is convenient to follow the guidelines for (passwords/phishing).</td><td>0.775 |0.849</td><td></td><td></td><td></td></tr>
<tr><td>SE3</td><td>I am able to follow the guidelines without much effort for (passwords/phishing).</td><td>0.927 |0.915</td><td></td><td></td><td></td></tr>
<tr><td>SE4</td><td>It is a simple thing for me to follow the guidelines for (passwords/phishing).</td><td>0.974 |0.883</td><td></td><td></td><td></td></tr>
<tr><td colspan="6"><b>Intentions</b> (Boss et al., 2015)</td></tr>
<tr><td>INT1</td><td>I intend to follow the guidelines for (passwords/phishing) right after this training.</td><td>0.874 |0.830</td><td>0.942 | 0.923</td><td>0.842 | 0.800</td><td>0.940 | 0.932</td></tr>
<tr><td>INT2</td><td>I predict I will follow the guidelines for (passwords/phishing) right after this training.</td><td>0.920 |0.908</td><td></td><td></td><td></td></tr>
<tr><td>INT3</td><td>I plan to follow the guidelines for (passwords/phishing) right after this training.</td><td>0.962 |0.942</td><td></td><td></td><td></td></tr>
</table>

Table C3. Correlation between covariates (Password | Phishing).

	REWARD	COST	SE	INT
REWARD	**0.731 | 0.792**			
COST	0.673 | 0.624	**0.761 | 0.781**		
SE	−0.484 | −0.477	−0.578 | −0.630	**0.867 | 0.872**	
INT	−0.401 | −0.418	−0.463 | −0.611	0.683 | 0.666	**0.919 | 0.894**

Square root of the AVE on the diagonal.

Appendix D: survival analysis

We performed a survival analysis on the length of time required to crack each password. We used a Kaplan–Meier method (Kaplan & Meier, 1958) (also known as the product-limit method) to examine the effect of susceptibility claims on the length of time required to crack a password. A log-rank comparison (Mantel, 1966) between high susceptibility and low susceptibility conditions did not reveal any significant differences between conditions $\chi^2(1, N = 138) = 1.224, p = .269$.