You've been Phished! The Effect of Threat Susceptibility in Fear Appeal Messages on Employee Security Training Motivation and Learning

Shadi Shuraida
TELUQ University
shadi.shuraida@teluq.ca

Abstract

Despite the importance of information security training programs, employees often lack the motivation and engagement to participate in these initiatives. On the other hand, the information security literature has examined the motivational effect of fear appeals (persuasive messages) on individuals' protective behaviors. It is thought that the perceived level of threat severity and susceptibility communicated in fear appeals arouse fear, thereby motivating individuals to protect themselves from the threat. The present study compared the effect of high and low threat susceptibility in fear appeal messages on employees' information security training behavior and subsequent protective behaviors. The results suggest that employees who were subjected to a higher threat susceptibility message were more likely to complete the suggested training, and when trained, were less likely to fall victims to a simulated phishing attack compared to those who completed the training in the low susceptibility group.

Keywords: SETA, information security training, fear appeal, threat susceptibility, phishing.

1. Introduction

Over the last few years, there has been a significant increase in organizational information security (ISec) breaches that are largely attributed to non-compliant information system (IS) use by employees. It is estimated that over 50% of organizational security incidents result from employee non-compliance with ISec policies (Khando et al., 2021). The most common threat to organizational ISec often comes from uninformed employees who fall victim to phishing attacks, which are estimated to have increased significantly over the last decade (Frank et al., 2022).

To address phishing threats, organizations rely on technical and non-technical countermeasures to detect and prevent phishing attacks (Aleroud & Zhou, 2017; Alkhalil et al., 2021; Sadiq et al., 2021). The technical countermeasures consist of techniques that are designed to detect and block phishing attacks according to their content or source (Alkhalil et al., 2021). While these technical measures mitigate the risk of phishing attacks, they are not 100% effective (Vega et al., 2022) as is evidenced by the high number of phishing attacks (IC3, 2021). Consequently, organizations turn their attention to employee actions and invest considerable sums and resources in information security education, training and awareness (SETA) programs to reduce employees' susceptibility to security threats in general (Alshaikh et al., 2019) and phishing attacks in particular (Hillman et al., 2023). Yet despite these efforts, the number of reported security breaches continues to rise, which may suggest that existing SETA programs are not effective in motivating (Barlow et al., 2018; Cram & D'Arcy, 2023) or improving employees' information security awareness (Alshaikh et al., 2018; Frank et al., 2022; Khando et al., 2021). To address employees' susceptibility to ISec threats, researchers have largely followed two streams.

The first stream has focused on managers' need to craft better communication messages that induce employees' compliance with ISec policies, (Barlow et al., 2018; Johnston et al., 2015). Most notably, researchers in this stream examined the use of persuasive messages (fear appeals) to incentivize and promote users' compliance with information security protection behaviors (e.g., Boss et al., 2015; Johnston & Warkentin, 2010; Johnston et al., 2015; Lowry et al., 2023; Park et al., 2021; Schuetz et al., 2020; Wall & Buche, 2017). Using protection motivation theory (PMT), fear appeal research in IS has focused on messages that highlight a threat and the person's ability to adaptively respond to that threat (Boss et al., 2015; Lowry et al., 2023). Previous ISec research using fear appeals has mainly used PMT to examine organizational employees' compliance with advice regarding a protective behavior such as backing up

URI: https://hdl.handle.net/10125/109388
978-0-9981331-8-8

their data (Boss et al., 2015), using anti-malware (Boss et al., 2015) and anti-spyware software (Johnston & Warkentin, 2010; Schuetz et al., 2020), changing passwords (Park et al., 2021), using strong passwords and sharing computer passwords (Barlow et al., 2018), or encrypting their data (Johnston et al., 2015).

On the other hand, ISec researchers have consistently argued and demonstrated that employees' security behaviors and compliance is determined by their security knowledge and awareness (Breitner et al., 2014; Bulgurcu et al., 2010; Puhakainen & Siponen, 2010; Siponen et al., 2010). Hence, the second stream suggests that organizations need to develop better security training methods and approaches to improve employees' awareness and response to information security threats (e.g., Alshaikh et al., 2018; Alshaikh et al., 2019; Jampen et al., 2020; Jensen et al., 2017; Kam et al., 2021; Kweon et al., 2021; Yeoh et al., 2021). It is thought that well-designed training initiatives will provide employees with the necessary knowledge that allows them to respond appropriately to information security threats (Al-Daeef et al., 2017). Although ISec training effectively enhances users' security behaviors (Alshaikh et al., 2019; Hakami & Alshaikh, 2022; Kumaraguru et al., 2007; Kumaraguru et al., 2010), these programs often fail due to employees' lack of motivation and engagement with the training (Silic & Lowry, 2020). The training sessions often interfere with employees' work tasks and therefore compete for their limited attention (Alshaikh et al., 2018; Cram & D'Arcy, 2023; Kumaraguru et al., 2007; Kumaraguru et al., 2010; Silic & Lowry, 2020). In addition, most employees do not consider security as part of their work, and are therefore not concerned with information security training (Alkhalil et al., 2021; Silic & Lowry, 2020). Hence, there is a need for more empirical studies need to examine methods that can motivate employees to participate and engage in ISec training initiatives.

The present research takes a first step towards in addressing this issue by examining the effect of different fear appeal messages on employees' motivation to undertake information security training, and their subsequent information security protective behaviors. To our knowledge, one study (Schuetz et al., 2020) has examined the effect of different fear appeal messages on users' intention to learn clues that identify spear-phishing, but did not measure users' ensuing protective behaviors against this threat.

Hence, drawing on protection motivation and expectancy-value models (Boss et al., 2015; Johnston et al., 2015; Lowry et al., 2023; Rogers, 1983; Witte & Allen, 2000), the objective of this study is to *empirically compare the effect of two fear appeal messages with varying threat susceptibility levels (high and low), on employees' ISec training and subsequent protection behaviors*. The results of a field experiment found that employees exposed to a high threat susceptibility message were more likely to complete the recommended ISec training. Moreover, trained employees from this group were less likely to fall victim to a phishing attack compared to those in the low susceptibility group who also completed the training.

2. Theoretical background and hypotheses

There is agreement between researchers and practitioners regarding the importance of ISec training programs on employees' information security knowledge and compliance (Alshaikh et al., 2018; Hakami & Alshaikh, 2022; Puhakainen & Siponen, 2010). Yet, despite their importance, employees have little incentive to participate in these initiatives that are often seen as a secondary task or a 'waste of time,' (Alshaikh et al., 2018; Cram & D'Arcy, 2023; Kumaraguru et al., 2007; Kumaraguru et al., 2010). Further, even when employees participate in these programs, they do not necessarily pay attention to the training and learn how to effectively protect themselves (Hillman et al., 2023; Kumaraguru et al., 2007; Kumaraguru et al., 2010; Silic & Lowry, 2020).

To explain employees' motivation to engage in secure behaviors, previous ISec research has primarily used protection motivation theory (PMT) (Boss et al., 2015; Lowry et al., 2023; Schuetz et al., 2020). Originating in health research, PMT was developed to explain the effect of fear appeals – persuasion communications – on individuals' attitudes and behaviors towards protecting themselves from a perceived threat (Floyd et al., 2006). PMT suggests that fear appeal messages trigger a threat appraisal and a coping appraisal process, which in turn determine individuals' motivation to engage in the recommended protective behavior from the threat (Floyd et al., 2006; Maddux & Rogers, 1983; Rogers, 1983; Witte & Allen, 2000). In this cognitive appraisal process, individuals first assess the threat in two ways: the threat severity (perception about the magnitude of harm) and threat susceptibility (perception about the probability of experiencing the threat). Then, if the individual perceives the threat as relevant, they will assess the coping mechanisms in terms of the efficacy of the recommended behavior in reducing the threat, and their own ability of performing the recommended behavior, i.e. their self-efficacy (Floyd et al., 2006; Witte & Allen, 2000).

Although PMT has been generally supported in ISec research, there have been inconsistent empirical findings regarding the effects of its individual constructs on protective ISec behaviors as a result of theoretical and empirical issues (Boss et al., 2015; Cram et al., 2019; Lowry et al., 2023; Mou et al., 2022). One potential issue is that few ISec studies manipulate fear appeal threats that allow discerning which variables make a fear appeal effective in arousing fear and ensuing protective behavior (Boss et al., 2015; Crossler et al., 2013; Mou et al., 2022; Schuetz et al., 2020).

The present study contributes to these literatures by manipulating threat susceptibility in fear appeal messages to examine its motivational effect on employees' learning protective behaviors. Further, it contributes to the ISec training literature by examining the effect of learning under both manipulations on employees' secure behaviors.

2.1. Threat susceptibility and protection motivation

Fear appeal messages are intended to influence individuals to adopt recommended behaviors, by informing them of the impending harm of a threat if they do not adopt these behaviors (Rogers, 1983). The objective of threats in fear appeal messages is to arouse enough fear in individuals that drive them to act according to the recommendations (Maddux & Rogers, 1983; Rogers, 1983; Witte, 1992). Consequently, if the threat is high (i.e., high severity and susceptibility) and individuals' believe they can successfully protect themselves (high coping efficacy), the more likely they will protect themselves from the danger and its negative consequences (Floyd et al., 2006; Maddux & Rogers, 1983; Witte, 1992). Further, it is believed that these three components, independently and in combination influence protective behaviors (Rogers, 1983).

Despite some contradictory findings regarding the motivating effect of threat susceptibility on protection motivation (Mou et al., 2022), the ISec literature has largely found a positive relationship between these two variables (Lowry et al., 2023). These findings confirm what has been found in the public health domain literature, which shows a medium to large effect between perceptions of threat susceptibility and protection motivation (Floyd et al., 2006; Lewis et al., 2007; Witte & Allen, 2000). In fact, some authors suggest that threat susceptibility has a larger impact on behavior change than perceptions of threat severity, arguing that a threat is more likely to be personally relevant to individuals who perceive themselves more susceptible to it (Lewis et al., 2007). As such, employees are more likely to follow the recommendation of undertaking the ISec training when they believe that they are more likely to experience the threat themselves. This motivates the first hypothesis:

Hypothesis 1: Employees who receive high threat susceptibility fear appeals are more likely to complete the ISec training (protection behavior) than employees who receive the low threat susceptibility fear appeals.

2.2. Threat susceptibility and learning

In addition to motivating individuals to protect themselves by undertaking the ISec training, it is also proposed that threat susceptability is also likely to increase individuals' attention, interest, and engagement with the ISec training, resulting in better protective behaviors against security threats. For one, there is a clear link in the literature between threats and increased attention (van Steenbergen et al., 2011). Accordingly, increased ISec threat susceptibility is likely to increase employees' attention to the training, resulting in better knowledge of how to identify and respond to phishing attacks.

Second, PMT is an expectancy-value theory in which susceptibility is an expectancy variable denoting the individual's perception of the probability that they will be exposed to the event (Rogers, 1983). If individuals perceive that they are more susceptible to an event that will affect their current or future goals, then they will regard it as personally relevant and significant (Priniski et al., 2018). In an organizational context, employees feeling susceptible to an ISec threat may view the potential consequences of these threats harmful to their professional goals. For example, employees may fear the threat of phishing attacks would lead to data loss that would impact their competence, image, or reputation. As a protective measure, employees would therefore perceive the task of learning protective behaviors against phishing attacks as a useful activity that connects with their professional goals, i.e., the task has a high utility-value. Based on utility-value models (Eccles & Wigfield, 2002; Hulleman & Harackiewicz, 2020), it can be expected that employees who feel susceptible to ISec threats will perceive the training as more important, thereby motivating them to become more deeply active and engaged in the training activity. This increased engagement is then expected to enhance their awareness and knowledge of ISec protective behaviors. Indeed, there is ample evidence in the education literature which supports this notion, and demonstrates the positive impact of interventions that promote utility-value perceptions on learning

outcomes such as knowledge and performance (Hulleman & Harackiewicz, 2020). In contrast, employees who feel less susceptible to ISec threats may overlook the relevance and value of the training to their current or future goals and are in turn less likely to be as engaged in the training task.

Hypothesis 2: Employees who receive high threat susceptibility fear appeals and complete the ISec training, are less likely to fall victim to a phishing attack compared to those in the low susceptibility group who also complete the training.

3. Methodology

A field experiment was conducted in a public medium-sized Canadian university. The experiment was conducted with the aid of the university's information security consultant as part of the university's routine simulated phishing campaigns. These campaigns are often run in organizations to assess and measure the susceptibility of the staff to phishing attacks, and in turn better hone training measures (Volkamer et al., 2020). Considering the results of these campaigns, the security consultant then sends out emails inviting members of the university to follow recommended security training modules.

This study was embedded in one of these simulated phishing and training initiatives, and was designed under the supervision of the university's information security committee whose members included the information security consultant, the university's IT Department Director, the Director of External Affairs and General Secretariat, and the study's author.

The study's design adhered to the ethical guidelines outlined by Finn and Jakobsson (2007) for conducting phishing experiments. Recognizing the importance and benefits of phishing research and the minimal risk to the participants, the university's ethics committee (IRB equivalent) approved to waiver participant consent for the study, with the agreement that the researcher obtain secondary access to anonymized data from the university's security consultant. More specifically, the researcher received a spreadsheet from the consultant with an anonymized list of participants, the manipulation they underwent, their staff position in terms of administrative or teaching, and their response behaviors to the phishing simulation. The ethics committee also considered that the simulated phishing attack was part of a routine program carried out by the IT department that collected the data, and therefore the researcher was not involved in the deceptive phishing attack, nor in the handling of employees' data.

The participants, procedure, and manipulations of the experiment are discussed in more detail below.

3.1. Participants

All 750 university employees were subjected to the simulated phishing attack. Out of those, 286 university administrative and teaching staff (169 admin, and 117 teaching, i.e., adjuncts and professors) were randomly drawn and assigned to one of two treatment conditions manipulating threat susceptibility: 1) high susceptibility fear appeal, and 2) low susceptibility fear appeal.

This process was done by the researcher who received an anonymized list of the randomly selected employees by the information security consultant. As such, no identifying information apart from administrative or teaching staff was provided to the researcher throughout the project. The security consultant provided demographic data about the two groups at the end of the experiment that is provided below in Table 1.

Table 1: Participant characteristics in each group

	Low susceptibility	High susceptibility
Female	93	89
Male	52	51
Age avg. (s.d.)	47.3 (11.4)	48.8 (10.8)
Years of org. experience (s.d.)	10.3 (8.7)	10.7 (8.6)

3.2. Procedure

Prior to conducting the phishing campaign, the security consultant agreed to not reveal the true nature of the experiment to participants who might contact him about the phishing attacks. In addition, to ensure employees take the fear appeal messages seriously, the Director of External Affairs and General Secretariat agreed to send the messages to the administrative staff, and the Director of Teaching and Research to send the messages to the teaching staff.

The study used a randomized block design with subgroups representing administrative and teaching staff. Accordingly, employees were randomly assigned from each block to one of the conditions. This resulted in 145 participants assigned to the low susceptibility condition (85 admin and 60 teaching), and 141 to the high susceptibility condition (84 admin and 57). Figure 1 shows the experimental procedure.

Figure 1. Experiment procedure and measures

Initially, the security consultant ran the routine simulated phishing campaign which included all of the university's employees. The phishing message simulated a shared drive file sent from an unverified address with the title of 'updated policy for all employees.' Individuals who clicked on this folder were directed towards a web page asking for their username and password. At this point, the employees' responses to the phishing attacks was recorded in terms of visiting the website (clicking on the link, or not clicking at all).

Then, about seven weeks following the simulated phishing campaign, a fear appeal message was sent via email to the 286 selected participants from the offices of the directors. 141 employees received the low susceptibility fear appeal message, while 141 received the high susceptibility one. At the end of the fear appeal messages (outlined in more detail below), the participants in both treatments were invited to follow two training modules which would enable them to identify phishing emails. Subjects' responses to these fear appeal messages was recorded in terms of completing the proposed security training modules or not.

Finally, seven weeks after the fear appeal messages were sent, a second simulated phishing campaign was run by the security consultant. This second phishing message simulated a message from the university's email provider asking users to click on a link to verify their accounts for added security. Participants' protection behaviors in terms of clicking on the link or not responding to it was then measured to evaluate their learning.

3.3. Manipulations

The messages used in both manipulations were constructed according to the ISec literature in terms of (1) identifying the threat and its severity, (2) outline the efficacy of a recommended response, and (3) the ability to take action (Boss et al., 2015; Johnston & Warkentin, 2010). More specifically, the messages outlined the widespread and serious and threat of phishing attacks, that compromise victims' accounts and may result in loss of data, reputation damage, identity theft, and malware infections on their systems (threat susceptibility and severity). They were also informed that the best way to protect oneself is to learn how to identify phishing emails, and that research has shown that users who learned to identify the indicators distinguishing phishing emails were unlikely to be phishing attack victims (response efficacy). At the end of the message, the participants in both treatments were invited (not obligated) to follow two new 'micro-training' modules of less than five minutes in total which would enable them to identify phishing emails.

Threat susceptibility was manipulated in the high group by including a sentence at the beginning of the message saying that they had been the victims of a simulated phishing attack in the previous weeks. This message was not included in the low susceptibility message. The messages used in both manipulations are provided in the appendix.

4. Data analysis and results

Before testing H1, the influence of the different manipulations (high vs. low threat susceptibility in fear appeal messages) on employees' protection motivation behavior (following the recommended training) was explored. The descriptive statistics shown in Table 2 suggest that more subjects in the high susceptibility group (32.6%) were more likely to complete the suggested training than in the low susceptibility group (22%).

Table 2: Subjects' training behavior in both manipulations

		Completed training		
		Yes	No	Total
Susceptibility	High	46	95	141
	Low	32	113	145

A chi-square test of independence was performed using SPSS v29, and showed a significant difference between both manipulations, $\chi 2$ (1, N = 286) = 4.02, p = .045. This result supports H1, such that employees who received the high threat susceptibility fear appeal message, were more likely to complete the training module than those who received the low threat susceptibility fear appeal message.

With regards to H2, it explores whether there was a difference in the subjects' actual protective behaviors with regards to the phishing threat in the different manipulations. The descriptive statistics shown in Table 3 below suggest that subjects who completed the training in the high susceptibility group, were less likely to fall victims to the second phishing campaign than those in the low susceptibility group who completed the training (0 individuals, or 0% of the high susceptibility group vs. 4 individuals, or 12.5% of the low susceptibility group).

Table 3: Protective behavior of subjects who completed training in both manipulations

		Clicked on link in 2nd phishing campaign		
		Yes	No	Total
Susceptibility	High	0	46	46
	Low	4	28	32

A chi-square test of independence was performed using SPSS v29, and showed a significant difference between both manipulations, $\chi 2$ (1, N = 78) = 6.06, p = .014. This result supports H2, indicating that employees in the high threat susceptibility message who completed the training, were more likely to follow the protective measures than those who followed the training in the low threat susceptibility message.

To ensure this finding was the result of learning from training, and not an effect of awareness difference between the two groups, a chi-square test was performed to examine the difference in protective behavior (clicking on 2nd campaign phishing link) between both groups (high vs. low susceptibility). The test did not show a significant difference between both groups in terms of protective behavior (clicking on 2nd campaign phishing link), $\chi 2$ (1, N = 286) = 0.18, p = .67.

Further, additional an additional test was conducted to explore if there were any initial knowledge differences between both groups. As such, a chi-square test was performed to examine the difference between both groups behaviors in terms of clicking on the phishing link during the first campaign (prior to receiving fear appeal message). This test also did not show any significant difference between both groups' clicking behavior in the first phishing campaign, $\chi 2$ (1, N = 286) = 0.024, p = .88.

These findings support the notion that employees who completed training in the high susceptibility group learned more than those in the low susceptibility group.

5. Discussion

The present study used a field experiment to compare the effect of high vs. low threat susceptibility fear appeal messages on employees' training motivation and ISec protective behaviors. The results showed that organizational employees who receive high susceptibility fear appeal message, are more likely to complete the recommended training than employees who receive the low susceptibility fear appeal message. These results are consistent with the findings of previous research using PMT (Floyd et al., 2006; Lowry et al., 2023), supporting the notion that higher threat appraisal increases individuals' protection motivation behavior. Further, the present study heeds the call to improve ISec research using PMT by manipulating fear appeal messages (Boss et al., 2015; Mou et al., 2022; Schuetz et al., 2020). Such manipulations are likely to shed light on theoretical and empirical issues in this line of research, and enable academics and practitioners alike to identify which fear appeal message characteristics would be effective in a given ISec context (Boss et al., 2015).

In addition, our findings also show that when employees who receive the high susceptibility message complete the training, they are less likely to fall victims to the simulated phishing attack than employees who receive the low susceptibility message and complete the training. This is an important contribution which suggests that employees' mental state regarding the security threat influences their view of the training task and their learning. This finding is significant to the ISec education and training literature and suggests that developing effective ISec training programs should consider learners' cognitive and affective processes. This finding is also consistent with previous social and cognitive learning theories which argue that learners' mental states influence the way they carry out a task and the resulting outcomes (Bandura, 1977; Eccles & Wigfield, 2002; Hulleman & Harackiewicz, 2020).

5.1. Limitations and future research

While the field experiment with actual employees provides high ecological validity, it presents an uncontrolled environment that potentially presents confounding factors. One example of this is that shortly after the first phishing simulation attack, some members of the university were targeted by an actual phishing attack, to which the security consultant sent out an informative message to all university employees about the threat. While this may have increased employees' awareness with regards to phishing attacks, there was still a statistically significant difference in the outcomes of both groups which can only be explained as the result of the experimental manipulations. Nevertheless, future research should replicate the effects of high and low susceptibility threat messages in a controlled experiment.

Another important limitation of this study is that employees' fear as a result of the fear appeals was not measured. Given the central role fear has on protection motivation, this goes against the recommendation in the ISec literature (Boss et al., 2015; Lowry et al., 2023). However, measuring employees fear would

have most likely increased employees' awareness to phishing attacks, and influenced their responses to the second phishing simulation. This would have likely confounded the results relating to employees' training and protection behaviors. Another issue related to fear is identifying the source of employees' fear. ISec researchers have questioned the relevance of fear in organizational contexts, arguing that ISec threats are not personally relevant (Johnston et al., 2015; Warkentin et al., 2016). Future research could extend the present study to examine if employees fear is with regards to their assets (e.g., data or hardware), to their professional status or reputation, or to their future career goals.

Another interesting future avenue for research would be to explore the cognitive mechanisms that influenced employees learning in each manipulation. For instance, did high threat susceptibility increase employees' interest (Hidi, 2006), cognitive attention (Ocasio, 1997), or their effort and time spent on the training (Wigfield & Eccles, 2000).

6. References

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017, July 5-7). Security awareness training: A review. World Congress on Engineering, London, U.K.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160-196.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018, January 3-6). An exploratory study of current information security training and awareness practices in organizations. Hawaii International Conference on System Sciences (HICSS 51), Hawaii.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019, June 8-14). Toward sustainable behaviour change: an approach for cyber security education training and awareness. 27th European Conference on Information Systems (ECIS),, Stockholm & Uppsala, Sweden.

Bandura, A. (1977). *Social learning theory*. Prentice Hall.

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*, 689-715. https://doi.org/10.17705/1jais.00506

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

Breitner, M., Hohler, B., Neumann, M., Uffen, J., & Lebek, B. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. https://doi.org/10.1108/mrr-04-2013-0085

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

Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy. *Information Systems Journal*, *33*(6), 1396-1422. https://doi.org/10.1111/isj.12460

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, *43*(2), 525-554. https://doi.org/10.25300/misq/2019/15117

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Eccles, J. S., & Wigfield, A. (2002). Motivational beliefs, values, and goals. *Annual review of psychology*, *53*(1), 109-132.

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology and Society Magazine*, *26*(1), 46-58.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2006). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Frank, M., Wagner, N., & Ranft, L. M. (2022). Who gets phished? Insights from a Contextual Clustering Analysis Across Three Continents. European Conference on Information Systems, Timosoara, Romania.

Hakami, M., & Alshaikh, M. (2022). Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study. *International Journal of Computer Science & Network Security*, *22*(4), 299-309. https://doi.org/10.22937/IJCSNS.2022.22.4.37

Hidi, S. (2006). Interest: A unique motivational variable. *Educational Research Review*, *1*(2), 69-82. https://doi.org/10.1016/j.edurev.2006.09.001

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, *132*. https://doi.org/10.1016/j.cose.2023.103364

Hulleman, C. S., & Harackiewicz, J. M. (2020). The utility-value intervention. In G. M. Walton & A. J. Crum (Eds.), *Handbook of wise interventions: How social psychology can help people change* (pp. 100-125). Guilford Press.

IC3. (2021). *Internet Crime Report*. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, *10*(1). https://doi.org/10.1186/s13673-020-00237-7

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.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly*, *39*(1), 113-134.

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2021). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, *32*(4), 888-926. https://doi.org/10.1111/isj.12374

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*. https://doi.org/10.1016/j.cose.2021.102267

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit,

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), 1-31.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, *23*(2), 361-373. https://doi.org/10.1007/s10796-019-09977-z

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.

Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. J. (2023). Examining the Differential Effectiveness of Fear Appeals in Information Security Management Using Two-Stage Meta-Analysis. *Journal of Management Information Systems*, *40*(4), 1099-1138. https://doi.org/10.1080/07421222.2023.2267318

Maddux, J., & Rogers, R. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology*, *19*, 469-479.

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach in Search Advertising. *Journal of the Association for Information Systems*, *23*(1), 196-236. https://doi.org/10.17705/1jais.00723

Ocasio, W. (1997). Towards an attention-based view of the firm. *Strategic Management Journal*, *18*(S1), 187-206.

Park, J., Son, J.-Y., & Suh, K.-S. (2021). Fear appeal cues to motivate users' security protection behaviors: an empirical test of heuristic cues to enhance risk communication. *Internet Research*, *32*(3), 708-727. https://doi.org/10.1108/intr-01-2021-0065

Priniski, S. J., Hecht, C. A., & Harackiewicz, J. M. (2018). Making Learning Personally Meaningful: A New Framework for Relevance Research. *J Exp Educ*, *86*(1), 11-29. https://doi.org/10.1080/00220973.2017.1380589

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757-778.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychology: A source book* (pp. 153-176).

Sadiq, A., Anwar, M., Butt, R. A., Masud, F., Shahzad, M. K., Naseem, S., & Younas, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. *Human Behavior and Emerging Technologies*, *3*(5), 854-864. https://doi.org/10.1002/hbe2.301

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*(1), 129-161.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer - IEEE Explore*, *43*(2), 64-71.

van Steenbergen, H., Band, G. P., & Hommel, B. (2011). Threat but not arousal narrows attention: evidence from pupil dilation and saccade control. *Front Psychol*, *2*, 281. https://doi.org/10.3389/fpsyg.2011.00281

Vega, J., Shevchyk, D., & Cheng, Y. (2022). *A literature survey of phishing and its countermeasures.* Second Annual Computer Science Conference for CSU Undergraduates.,

Volkamer, M., Sasse, M. A., & Boehm, F. (2020, September 17–18, 2020). Analysing simulated phishing campaigns for staff. Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK.

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

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

Wigfield, A., & Eccles, J. S. (2000). Expectancy-Value Theory of Achievement Motivation. *Contemp Educ Psychol*, *25*(1), 68-81. https://doi.org/10.1006/ceps.1999.1015

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

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: implications for effective public health campaigns. *Health Educ Behav*, *27*(5), 591-615. https://doi.org/10.1177/109019810002700506

Yeoh, W., Huang, H., Lee, W.-S., Al Jafari, F., & Mansson, R. (2021). Simulated Phishing Attack and Embedded Training Campaign. *Journal of Computer Information Systems*, *62*(4), 802-821. https://doi.org/10.1080/08874417.2021.1919941

Appendix – Fear appeal messages used in the experimental manipulations[1]

Below is the text used in the fear appeal messages. While the messages in the two treatments were identical, the first paragraph (in italics) was only included in the high susceptibility manipulation.

"Over the past few weeks, we have been running a phishing simulation as part of the information security program. We have also been the victim of a real phishing campaign originating from within our infrastructures.

Phishing attacks are one of the most widespread and dangerous forms of cybercrime. Phishing messages adopt common, familiar patterns to make them appear genuine. The aim is often to obtain your personal information or passwords to commit fraud or identity theft. These attacks can result in data loss, compromised accounts or credentials, reputational damage or malware infections, including ransomware.

The best way to avoid falling victim to phishing is to learn how to spot a phishing email. There are many clues that an e-mail is fake. Research has shown that users who have learned to recognize these clues are less likely to fall victim to phishing attacks.

[The university] is currently deploying a cybersecurity awareness platform, and you are among the first to have access to it. We invite you to take two micro-training sessions, each lasting less than 5 minutes. The connection information to this training follows this message."

[1] Fear appeal message translated by the author from French.