Fear might motivate secure password choices in the short term, but at what cost?

Marc Dupuis
University of Washington
marcjd@uw.edu

Karen Renaud
University of Strathclyde
karen.renaud@strath.ac.uk

Anna Jennings
University of Washington
annajennings1@acm.org

Abstract

Fear has been used to convince people to behave securely in a variety of cybersecurity domains. In this study, we tested the use of fear appeals, together with threat and coping appraisal components separately and together, on password hygiene behaviors. Fear did indeed elicit the anticipated response: people had higher levels of behavioral intention to engage in better password hygiene. Unfortunately, we also detected a largely negative affective response to the appeals. Fear, as a short-lived emotion, can indeed be effective in the short term. Snapshot-like studies, like the one reported here, might lead us to conclude that fear is indeed indicated and efficacious. Yet, it may backfire in the long term due to the negative long term affects it can trigger.

1. Introduction

Passwords have been used to authenticate humans since we started using computers, while fear appeals have been around for centuries. Fear has been used by religions, in public health messaging, and latterly in cybersecurity to persuade people to change their behaviors [1]. All of these efforts take the efficacy of fear, as a behavioral change tool, for granted. This might be because people often *do* respond to fear, visibly taking the actions they are coerced into taking.

Even so, it is rare for anyone to consider the empirical evidence attesting to the long-term power or limitations of induced fear. Might fear merely *appear* to work, being a palliative instead of an intervention? Does fear lead to permanent behavioral change? Might the short-term changes in behavior subsequent to administration of a fear appeal be misleading us? These are questions that beg to be answered.

An example of the negative consequences of fear appeals are manifesting in the United Kingdom (UK). The UK government's Behavioural Insights Unit actively advised the government to utilize fear in order to persuade the British public to comply with lockdown and other pandemic regulations [2]. This use of fear achieved its aims: the British public accepted the initial lockdown, and the many extensions that occurred over the following 15 months. Vaccine uptake has been exemplary. Yet, a number of negative consequences are now emerging and the UK public are the most frightened of COVID in the world[1]. Such levels of anxiety cannot be healthy or desirable. Dodsworth makes a strong argument that fear "should not be weaponised" arguing that this particular emotion, when weaponized, creates a great deal of collateral damage.

We set out to determine whether Dodsworth's admonition also applies to the use of fear in the cyber domain. We focus on the use of fear in encouraging better password hygiene. This is to help us determine how, when, where, why, and in what context fear appeals may be most effective, desirable, and ethical [3, 4]. In this study, we employed a randomized controlled between-subjects design with three treatment groups to test the efficacy of fear appeals in changing behavioral intentions with respect to three password hygiene behaviors.

We found that fear did indeed lead to stronger passwords. However, it also led to higher levels of negative types of state affect for the two groups that were exposed to the fear component, as compared to the two groups that did not receive the fear appeal. Section 2 reviews related research. Section 3 describes the methods we used, with Section 4 identifying the materials employed. Section 5 reports on the findings with Section 6 discussing them and limitations. Section 7 concludes and suggests future work.

2. Related Research

2.1. Affect

Throughout the literature, affect has been defined and articulated in a number of ways. It has often been used interchangeably with mood and emotion (e.g.,

[1] https://www.telegraph.co.uk/news/2020/05/05/britons-scared-coronavirus-infection-rest-world/

URI: https://hdl.handle.net/10125/79922
978-0-9981331-5-7

[5, 6]). Although this is understandable given their interdependence, it can make it challenging when one study may mean something quite different than another with respect to the use of these terms.

In the current study, emotion can be viewed as a short-lived and relatively intense reaction to a stimulus. Emotion may vary significantly over relatively short time periods. It may eventually become mood, which will depend on the frequency, intensity, and context of the experienced emotion(s). In contrast, mood is viewed as longer-lasting and milder in intensity [5].

Both emotion and mood are considered affective states [6]. Examples of affective states include: guilt, hostility, fear, fatigue, surprise, sadness, attentiveness, serenity, shyness, joviality, and self-assurance [7]. However, in addition to affective states, there is also trait affect, which represents a generally more stable and life-long type of affect that changes very little over time, similar to personality in many respects [8].

Differences in persistence is one way in which different types of affect may vary from one another. However, affect may also vary in the extent to which it is related to the decision at hand or in response to a specific stimulus. Incidental affect is a type of affect that is not related to the current judgment or stimulus, but can still influence it [9]. While trait affect is always an incidental type of affect, emotion and mood may or may not be incidental, depending on the particular circumstances.

In contrast to incidental affect, integral affect is relevant to the current choice, judgment, or stimulus [9, 6]. This is seen when someone anticipates regretting a decision, such as betting on a team. This may result in a change in their betting behavior, influencing the size of the wager [10]. Loewenstein *et al.* [11] has termed this 'anticipated emotion'. Anticipatory emotions, on the other hand, include immediate visceral reactions to threats (e.g., fear) [11]. Both anticipatory and anticipated emotions are considered types of integral affect as they are directly related to, and triggered by, the current judgment or stimulus.

2.2. Fear Appeals

Fear is invoked when a threat exhibits a number of characteristics: (1) it is important to the person, (2) it is negatively valenced, (3) the threat is impending, and (4) it requires the person to engage in some kind of effort to offset the threat with a recommended action [1]. Fear, as an emotion, undoubtedly exerts an influence on humans [12], hence its appropriation as a behavioral change intervention across a range of domains.

Fear is used in behavioral change interventions in the belief that the elicited fear will convince people to do what the fear appeal deployer wants them to do [12]. The idea is that they will take action in order to reduce levels of fear.

Renaud and Dupuis [1] reviewed the use of fear appeals in the cybersecurity domain. They reported that the majority of the studies take a snapshot, presenting participants with a fear appeal and then asking a number of questions. Some observed subsequent behaviors. Very few studies returned to the participants after a significant period of time to determine the whether the impact of the fear appeal endured. None checked that the recommended behavior the fear appeal was trying to trigger was feasible to the recipient.

A number of the studies reviewed by Renaud and Dupuis [1] used fear to strengthen passwords [13, 14, 15, 16]. These generally reported that the fear appeals were effective, but most measured behavioral *intention* via a survey question or via self-report. Likewise, very few measured the level of fear that may have been induced, let alone other more enduring emotions.

One of the exceptions with respect to the measurement of fear was Boss *et al.* [17], who adapted items from Milne *et al.* in reporting their first study [18]. The underlying assumption was that fear was being measured. However, the origin of the items they used was not provided by Milne *et al.*, nor was any information provided with respect to the development and validation (i.e., construct validity) of these items [18]. The four items used to measure *fear* included the descriptors 'worried', 'frightened', 'anxious', and 'scared'. In their second study, they adapted items from Osman *et al.* [19], which was an examination of an instrument originally designed by McCracken *et al.* [20]. However, the original subscale that examined fear included 10 items, while Boss *et al.* used six. It is also worth noting that the original instrument, the Pain Anxiety Symptoms Scale (PASS), was developed to measure the fear of *pain*. The fear of something real physiologically (i.e., pain) and not abstract (i.e., security [21]), may not be the same thing. Hence, measuring them in the same manner may not be appropriate. Despite any possible issues with how fear was measured in their studies, they did find that fear could be elicited and measured within the context of a fear appeal study. This should be the rule rather than the exception in carrying out these kinds of studies.

Another study suggests that how a fear appeal is deployed may make a difference in its efficacy. Vance *et al.* examined the use of four different types of password interfaces: 1) control; 2) interactive password strength meter; 3) static fear appeal treatment, and 4) interactive fear appeal treatment [22]. The interactive fear appeal messaging was the only treatment that demonstrated significant improvement in password creation. The reason for this is later delineated in Vance *et al.* [23]. While the secondary nature of many security tasks has long been recognized (e.g., [21]), the primary or secondary nature of fear appeals while performing security tasks has not been closely examined prior to [23]. They articulate the role of engagement with the fear appeal and how it is already high when the fear appeal is part of a primary task, but inherently low when that task or the appeal itself is secondary in nature. By increasing the level of engagement between the end user with the fear appeal, higher degrees of success will be found in either type of task, but will perhaps be most pronounced in secondary tasks where engagement has a low baseline.

The dynamic deployment of fear appeals was also found to be quite effective by Jenkins *et al.* [24]. Similar to Vance *et al.*'s, feedback in the form of a fear appeal was provided immediately as characters were entered into the keyboard during password creation. Their focus was on password reuse. 88.41% of participants that received the fear appeal choosing to create a unique password compared to only 4.45% of those that did not receive the fear appeal. Thus, within the cybersecurity domain there may be opportunities to provide immediate feedback in the form of a fear appeal and such feedback may be highly effective. Passwords lend themselves to such immediate feedback, while other protective behaviors in cybersecurity may be more difficult to replicate in a similar manner (e.g., back-ups of data).

2.3. Protection Motivation Theory

Fear appeals have been used for centuries and have been examined using a range of theoretical approaches designed to better understand human behavior, including Protection Motivation Theory (PMT) [25]. PMT helps explain why some individuals may engage in a recommended action with the purpose of reducing the threat, while others may be more concerned with reducing the level of fear they may feel, engaging in 'danger control' rather than 'fear control'.

Rogers developed PMT in 1975 as an extension of expectancy-value theory [26]. Self-efficacy was later added to the theory, given its role in successfully accounting for one's willingness to engage in a specific behavior [27, 26]. PMT consists of threat appraisal and coping appraisal. Threat appraisal consists of the constructs: 'perceived threat severity', 'perceived threat vulnerability', and 'rewards', the latter of which has rarely been used in practice [28]. Coping appraisal consists of the constructs 'self-efficacy', 'response efficacy', and 'response costs' [29]. The threat appraisal and coping appraisal components are examined separately and then together in this study. The context in which this is done is by examining the threat of having one's passwords compromised.

2.4. Passwords

Most users prefer passwords over alternative authentication mechanisms, probably due to their familiarity and the ubiquity of text entry mechanisms [30]. Other authentication types, such as biometrics or tokens, often involve extra expense or additional hardware, and are sometimes error-prone. Hence, passwords are the most popular authentication mechanism for both end users and developers [31].

The rules related to the format of the password are generally simple, but vary considerably in their implementation from one program or application being used to another. These authentication systems usually specify a minimum length of the password, complexity requirements, and that they should be kept secure. However, there are few mechanisms in place to ensure an individual creates unique passwords. Likewise, most individuals do not use password managers to simplify such requirements and/or guidelines [32].

2.5. Research Model

The research undertaken here focuses on two objectives. *First*, to assess the degree to which different conditions presented to participants may impact the efficacy of the target behaviors within a PMT model. *Second*, to determine whether it is fear by itself that is elicited or one or more other emotions.

For the *first* objective, and consistent with other research that has employed PMT within the information security domain (e.g., [33]), we propose the following five hypotheses:

H1: Higher levels of perceived threat *severity* related to having one's passwords compromised will be associated with higher levels of intent to perform the target password hygiene behaviors.

H2: Higher levels of perceived threat *vulnerability* related to having one's passwords compromised will be associated with higher levels of intent to perform the target password hygiene behaviors.

H3: Higher levels of *self-efficacy* related to performing the target password hygiene behaviors will be associated with higher levels of intent to perform the target password hygiene behaviors.

H4: Higher levels of *response efficacy* related to one's belief in the effectiveness the target password hygiene behaviors will be associated with higher levels of intent to perform the target password hygiene behaviors.

H5: Higher levels of *perceived response costs* related to performing the target password hygiene behaviors will be associated with lower levels of intent to perform the target password hygiene behaviors.

The *second* objective will be evaluated by comparing the mean values of the different groups for each of the higher order and lower order dimensions of state affect measured. Given the complexity inherent to emotions and the elicitation thereof, we expect participants that were exposed to a treatment that had a fear component to it would see increased levels of other negative emotions and decreased levels of positive emotions when compared to participants that were not exposed to a fear component. Therefore, we propose the following two hypotheses:

H6: Participants in experimental groups that received a fear component will have *higher levels of negative types of state affect* other than fear when compared to participants in the non-fear groups.

H7: Participants in experimental groups that received a fear component will have *lower levels of positive types of state affect* when compared to participants in the non-fear groups.

3. Methods

The current study measures self-reports of behavior before the treatment (or control) and then behavioral intentions after the treatment (or control) has been completed. Although this study does not address all of the issues raised by Renaud and Dupuis [1], an important contribution of this study is to separate the core components of a fear appeal into two distinct elements, threat appraisal components (perceived threat severity and perceived threat vulnerability) and coping appraisal components (self-efficacy, response efficacy, and response costs). Another important contribution is the examination of the specific types of state affect elicited within each of the four groups and how they compare to one another in this regard.

3.1. Participants

Prior to collecting data from participants, Institutional Review Board (IRB) approval was sought and obtained. Participants were recruited from Amazon's Mechanical Turk (MTurk) and the survey was hosted on the Qualtrics survey platform. Compared to other recruitment methods, MTurk has been shown to be both efficient and reliable with respect to participant recruitment so long as quality control measures are used, such as attention check questions [34, 35].

In the current study, two automated quality control questions were used. If a participant failed either of them then the survey would end with a message explaining that they had failed a quality control question. Additionally, toward the end of the survey we had an open-ended question that was also used as a *de facto* quality control measure. By sorting them in alphabetical order and reading through the responses provided, we are able to detect cases in which automation was likely used. Since each version of the survey required the participant to watch one of four different videos, we used a timing option within the Qualtrics survey platform to prevent individuals from advancing to the next question before a time equivalent to the length of the video had elapsed. Finally, we limited eligibility to participate in the survey to MTurk workers that had an approval rate of 98% or greater and had previously completed at least 1,000 HITs (human intelligence tasks).

A pilot study with 107 participants was used to reveal any problems with question wording and survey flow, as well as to ensure fair compensation for participants. No significant issues were detected and compensation for participants was set at $2.50. The compensation provided was considered fair given the responses provided to a compensation question included at the end of the survey with 91.2% of participants believing that the compensation provided was either comparable (69.9%) or easier for the money (21.3%) when compared to similar projects they had previously completed on MTurk with a small number (8.8%) believing that more effort was required in comparison.

Of the 811 participants that began the survey, 1.5% failed one of the quality control measures. As a result, there were 799 valid responses that were used for subsequent analysis. Participants were mostly evenly divided between the four groups based on a random assignment feature within Qualtrics: (1) Control (N=202); (2) Threat appraisal components only (N=201); (3) Coping appraisal components only (N=195), and (4) Combined threat and coping appraisal components (N=201).

Most participants stated they were White (77.2%), followed by Asian / Pacific Islander (8.4%), Black / African American (8.1%), Hispanic (4.3%), Other / Multi-Racial (1.6%), and Native American / Alaskan Native / Indigenous (0.4%). Approximately half of our participants identified as male (51.2%), followed by female (47.8%), non-binary or third gender (0.6%), or preferred not to say (0.4%). Most of the participants (54.9%) were 40 or older with the remaining participants (45.1%) between the ages of 18 and 39.

4. Materials

Existing instrumentation was used when possible. If this was not feasible, then previously developed and validated items were used and adapted for the current study. This included the questions related to the PMT constructs [36, 37, 18]. When this was not possible, measurement tools were developed and validated, such as the videos and the target password hygiene behaviors.

4.1. Objective 1: Password Hygiene Behaviors

As noted earlier, there is significant disagreement on the specific behaviors and practices one should engage in related to performing good password hygiene. Thus, the Delphi technique was employed with a group of 11 subject matter experts (SMEs) that engage in cybersecurity a majority of their time through a typical workday. The Delphi technique has been employed in information systems and cybersecurity based research before (e.g., [38] and is a common technique employed to reach consensus. Three rounds were performed with the first round being the most open. SMEs were able to provide their own ideas related to measures necessary for good password hygiene during the first round. The second round included these responses along with other measures found in the literature and from organizations.

Consensus became important during the second and third rounds. Significant disagreement was found for most of the items. Consensus was considered achieved if 75% or more of the SMEs were in agreement. This was based on both historical precedence and also finding a balance between some agreement (i.e., 50%) and complete agreement (i.e., 100%) [39]. Wording changes were made and clarity sought after the second round. The third round contained five remaining items: (1) Length; (2) Complexity; (3) Kept secure; (4) Unique, and (5) Changing passwords. Although most SMEs preferred passwords of significant length (15 or more characters), they also recognized the need to balance that with the usability challenge it may cause for the average consumer. Consensus was obtained with respect to length (10 characters long or longer), uniqueness, and the importance of keeping passwords safe and secure.

4.2. Objective 2: State Affect

There are advantages and disadvantages to measuring different types of affect in the context of a study. For the current study, our interest lies in how the condition presented to the participants resulted in specific emotional states. We are not interested in how they think from an affective perspective about the specific stimulus (i.e., the treatment), but rather how they feel in the immediate aftermath of having received the stimulus. Thus, we measured incidental state affect rather than integral state affect or trait affect. The PANAS-X scale was used with specific instructions provided to measure incidental state affect [7].

4.3. Embedded Videos

As part of the survey, participants were required to watch one of four different videos depending on the group to which they had been randomly assigned by the Qualtrics survey platform. These videos were developed and iterated upon based on feedback from undergraduate and graduate students as well as the pilot study. The lengths of the videos were kept short so as to maximize attention to the content. They varied in length from 2:05 (control, coping appraisal only) to 2:29 (threat appraisal only) and then 4:34 (combined threat and coping appraisal video). The videos can be accessed from: https://tinyurl.com/password-fear-appeal

For the **control group**, the goal was to develop a video that was neutral in tone and without a specific message. Instrumental music was combined with various short video clips, such as cars driving, scenery, sand in the desert, vegetation blowing in the wind, etc.

The **threat appraisal only** group received messaging that emphasized the severity of their passwords being compromised and their level of vulnerability. Several data breaches were presented, including the number of accounts impacted and how that may lead to passwords being compromised as a result. Other possible ways their passwords could be compromised was also presented, such as having their passwords cracked easily because they were too short in length.

The **coping appraisal only** group focused on the three target password hygiene behaviors: 1) length (10 characters long or longer); 2) Unique passwords for different websites and systems, and 3) Secure: the password should be kept safe and secure from others. A mnemonic was developed so that these three components would be easier for participants to remember. P-L-U-S: **P**asswords should be **L**ong, **U**nique, and **S**ecure. The three constructs from coping appraisal in PMT were emphasized: the steps an individual can take and how to take them (i.e., self-efficacy), the effectiveness of those steps (i.e., response efficacy), and the time, energy, and effort involved in taking those steps (i.e., response costs).

A brief demo of a password manager was given to demonstrate the efficacy and ease with which such a tool can address the three components presented to them. An additional measure was also included in this video: combining at least six or more unrelated words together as an approach to developing long passwords. The **combined** group saw a merged version of the video from groups two and three with threat appraisal followed by coping appraisal.

5. Results and Analysis

Analysis was conducted using IBM's Statistical Package for Social Sciences (SPSS) version 19.0 and SmartPLS version 3.3.2. The focus of our analysis is two-fold. First, we want to determine the extent to which the videos may have influenced our participants' behavioral intention to engage in creating long, unique, and secure passwords through an examination of four different PMT measurement model results. Second, we are interested in understanding to what extent the emotions elicited in the four groups vary.

5.1. Pre-Treatment Analyses

Prior to the treatment condition (or control) being presented to the participant, we asked them about their level of confidence that they currently perform the three password hygiene behaviors. A one-way between subjects ANOVA was performed to assess whether there was a significant difference between any of the four experimental groups in this study. None were found. This suggests that any effect found post-treatment was most likely due to the treatment itself.

5.2. Measurement Models

A single research method was used in this study: surveys. Common method bias (CMB) may result in such cases and should be tested for to determine if it is a significant issue or not. A test often used to screen for CMB is the Harman's single-factor test. While this test does have some shortcomings [40], it is helpful in identifying if CMB is an issue within a data set. Less than 16.1% of the total variance was explained by a single factor; this is below the maximum threshold of 50%. Although it is important to test for CMB after data has been collected, it is also important to design the study in such a way as to minimize the likelihood of it becoming a problem. In the current study, this was done by providing instructions to the participants that there are no right or wrong answers—to just answer honestly, as well as the use of Amazon's Mechanical Turk, which provides a high level of anonymity for research participants.

Cronbach's Alpha and composite reliability values were over the 0.700 minimum threshold, which suggests that reliability is acceptable for the reflective constructs used in the measurement models [41]. Additionally, convergent validity was also found acceptable with the composite reliability values greater than the AVE for all of the constructs and greater than the 0.500 minimum [41]. The measures also demonstrated discriminant validity as the AVE of the constructs were greater than the square of the correlations with other constructs; the cross-loading method of assessing discriminant validity was also done and was consistent with adequate discriminant validity [42]. Loading was greater for all of the indicators for their intended construct than any other construct. Discriminant validity was also assessed and supported by using The Heterotrait-Monotrait Ratio (HTMT) method [43].

The approach outlined in [44] was used to measure and model the multiple dimensions involved in the research model, which consists of reflective first-order, formative second-order constructs (self-efficacy, response efficacy, and response costs). Since there were three behaviors in this study, it was important to assess the coping appraisal components for each of them. For example, self-efficacy had three dimensions to it—one for each of the behaviors. Each of these dimensions were formative for the construct of self-efficacy and were measured individually using three reflective indicators that were adapted from the literature.

The five hypotheses were assessed using SmartPLS 3.3.2. In Table 1, we present the individual results for each of the four measurement models. Three of the four models only had two out of five hypotheses supported, while the combined fear and efficacy group had three out of five hypotheses supported. However, the amount of variance explained was the highest for the threat appraisal only group at 53%. Similar to other research [28], self-efficacy was consistently the best predictor of behavioral intent in these PMT models.

5.3. State Affect

In addition to evaluating the results to assess support for or against the hypotheses, we also evaluated state affect elicited from each of the four groups. Incidental state affect was measured using the PANAS-X [7, 8]. In Table 2, we provide the results of a one-way ANOVA test with Tukey HSD post-hoc analysis. The state affect dimensions that did not yield a statistically significant result are not included in the table.

Several interesting observations may be made from these results. *First*, there is a clear delineation in the types of state affect elicited in the groups that included a fear component versus those that did not. In each and every case in which the one-way ANOVA test showed significantly different results between these two types of

Table 1. PLS-SEM Results for the Four Groups

Group 1: Control; R^2 = 35.10%			
	T statistic	*P value*	*Supported?*
H1: TS	***2.121***	***0.017***	***Yes***
H2: TV	1.198	0.116	No
H3: SE	***4.63***	***p <.001***	***Yes***
H4: RE	0.17	0.433	No
H5: RC	0.914	0.180	No
Group 2: Threat Appraisal Only; R^2 = 53%			
	T statistic	*P value*	*Supported?*
H1: TS	1.621	0.053	No
H2: TV	0.734	0.231	No
H3: SE	***4.189***	***p <.001***	***Yes***
H4: RE	***3.479***	***p <.001***	***Yes***
H5: RC	1.323	0.093	No
Group 3: Coping Appraisal Only; R^2 = 37.30%			
	T statistic	*P value*	*Supported?*
H1: TS	1.45	0.073	No
H2: TV	0.033	0.487	No
H3: SE	***3.29***	***0.001***	***Yes***
H4: RE	0.076	0.47	No
H5: RC	***2.75***	***0.003***	***Yes***
Group 4: Combined; R^2 = 39.10%			
	T statistic	*P value*	*Supported?*
H1: TS	***1.701***	***0.044***	***Yes***
H2: TV	1.388	0.083	No
H3: SE	***3.189***	***0.001***	***Yes***
H4: RE	***1.906***	***0.028***	***Yes***
H5: RC	1.198	0.083	No

groups, the groups that used fear (i.e., threat appraisal) always elicited greater levels of negative affect and/or lower levels of positive affect.

Second, one of the most noteworthy issues raised in Renaud and Dupuis was the assumption that fear is elicited through fear appeals. This is assumed without attempting confirmation by measuring either fear or other emotions taking place [1]. These results demonstrate why we cannot take the elicitation of fear, and only fear, for granted. In the fear only group, hostility was elevated at significantly higher levels than either the control or coping appraisal only groups. Joviality is significantly lower for both groups that used fear as compared to the two groups that did not receive the threat appraisal messaging of a fear appeal. This pattern is also observed for state serenity. Therefore, hypothesis 6 is partially supported with three instances of a lower order dimension of state negative affect other than fear being elicited at a higher level when a fear component was included compared to when it was not. Likewise, hypothesis 7 is also partially supported with five instances of a lower order dimension of state positive affect being elicited at a lower level when fear was included compared to when it was not. Serenity is not considered a lower order dimension of either positive or negative affect [7].

Third, the differences noted here in the types and nature of the affect elicited were the likely result of watching very short videos of approximately two to less than five minutes in duration, depending on the specific video. However, even from that short encounter with fear used in two of the four groups, we see several instances of a variety of negative types of state affect elicited. What does this suggest for more pronounced fear appeal efforts, including repeated negative messaging by an employer or the government?

6. Discussion

Dodsworth [2] argues that "*happy endings are not written in the language of coercive control.*" We discovered that the use of fear caused our participants to create stronger passwords. Yet, they also led to negative affect. When people experience negativity towards something, they are likely to avoid it: to be reluctant to engage enthusiastically with the password creation process in the future [45]. We have to wonder what the consequences of this negative affect will be in a week, a month or a year. Moreover, what will the impact be on their general well-being [46]?

6.1. Implications

This study provides important insights into the use of fear appeals within the cybersecurity domain. It demonstrated that providing messaging on the nature of a threat (i.e., threat appraisal) and what can be done to address the threat (i.e., coping appraisal) may help engender behavioral change toward the targeted behavior(s). However, the extent to which this messaging is delivered (or not) influences the manner in which PMT may help explain their behavioral intentions. Other than perceived threat vulnerability, which has been problematic in much of the PMT literature, all of the hypotheses received at least some support in one or more of the four models. Fear appeals even lower in complexity than done here and with focus on a single recommended action can be effective, at least in the short term [17, 24]. This suggests that throwing the kitchen sink at end users may be too burdensome, and perhaps, as a result, less effective.

Additionally, the results on state affect suggest that affect needs to be measured on a more regular basis when fear is employed. Fear is rarely measured, despite the fact that a *fear appeal* is being used. To the

Table 2. Differences in Dimensions of State Affect in Fear and Non-Fear Conditions

Construct	Group A	Group B	Mean Difference (A-B)	Std. Error	Sig.
State Negative Affect ***F(3,795)=8.149, p<.001***	Threat Appraisal	Control	.29281*	.06531	.000
		Coping Appraisal	.24109*	.06589	.002
	Combined	Control	.18336*	.06531	.026
		Coping Appraisal	.13164	.06589	.190
State Fear ***F(3,795)=7.881, p<.001***	Threat Appraisal	Control	.31297*	.07018	.000
		Coping Appraisal	.24877*	.07080	.003
	Combined	Control	.19689*	.07018	.026
		Coping Appraisal	.13268	.07080	.240
State Hostility ***F(3,795)=4.943, p=.002***	Threat Appraisal	Control	.19764*	.06129	.007
		Coping Appraisal	.19722*	.06184	.008
	Combined	Control	.11887	.06129	.212
		Coping Appraisal	.11845	.06184	.222
State Guilt ***F(3,795)=3.283, p=.020***	Threat Appraisal	Control	.19168*	.06857	.027
		Coping Appraisal	.15698	.06918	.106
	Combined	Control	.13198	.06857	.218
		Coping Appraisal	.09728	.06918	.496
State Joviality ***F(3,795)=13.781, p<.001***	Threat Appraisal	Control	-.61638*	.10477	.000
		Coping Appraisal	-.44398*	.10570	.000
	Combined	Control	-.44660*	.10477	.000
		Coping Appraisal	-.27421*	.10570	.047
State Self-Assurance ***F(3,795)=3.336, p=.019***	Threat Appraisal	Control	-.26753*	.09405	.024
		Coping Appraisal	-.17394	.09489	.259
	Combined	Control	-.22027	.09405	.090
		Coping Appraisal	-.12667	.09489	.541
State Serenity ***F(3,795)=21.494, p<.001***	Threat Appraisal	Control	-.72639*	.10391	.000
		Coping Appraisal	-.60143*	.10484	.000
	Combined	Control	-.53734*	.10391	.000
		Coping Appraisal	-.41237*	.10484	.001

** The mean difference is significant at the 0.05 level.*

extent that fear and fear alone is measured, these results indicate that we may be missing a significant amount of the complicated picture on how other affective components are elicited from a fear appeal, whether positive or negative types of affect.

6.2. Ethical Considerations

In deploying fear in any cybersecurity context, it is important not to ignore ethical considerations. Dupuis and Renaud [3] proposed six ethical principles to guide cybersecurity fear appeal experiments and deployment. These are: (1) obtain IRB approval, (2) make the benefits of cybersecurity salient, (3) only use deception if it can be rigorously justified, (4) provide a feasible recommended action (with the implication that feasibility will be verified), (5) calibrate during deployment (with the implication that the option to cease and desist will be considered if undue negative consequences are evident), and (6) debrief targets of fear appeals. If the fear appeal cannot be used within these constraints, deployers should carefully re-consider going ahead with the use of fear appeals.

6.3. Limitations

There are several limitations worth noting. First, this was a single survey using a crowd-sourced participant pool. While compensation was considered fair by most, MTurk workers do have an incentive to complete the work as quickly as possible. Thus, some responses and their overall attention may not be optimal for the messaging being delivered.

Second, data was collected for this study via a survey and no other method. Thus, common method bias is a concern [47]. Multiple quality control procedures were implemented to help address this concern. Additionally, the participant population is essentially anonymous to the research team. Thus, while certain elements of the procedures employed and participant pool used help to minimize the likelihood that common method bias was a significant factor in the results obtained, it remains a concern nonetheless.

Third, the collected data comes from a single snapshot in time for our participants. This was not a longitudinal study and we do not know whether the difference in behavioral intentions lasted beyond the completion of the survey. Likewise, we do not know if the behavioral intentions themselves resulted in any actual change in behavior.

Finally, we do not know if any emotional harm resulted from the fear that was elicited. While this study was considered low risk and approved as exempt from a full IRB review, part of the challenge with using fear appeals is the balance between enhanced coping appraisal being offset by the possible harms that could result from being scared into doing something.

7. Conclusion

In a world in which we are constantly bombarded with fear to try and cause a change in behavior, it is important that we begin to understand the very nuanced nature of eliciting a specific emotion and how that may impact behavior and one's overall emotional state.

Is the use of fear appeals *worth it*? That is a difficult question that cannot be answered here. However, what we do know is that we should not take for granted that fear appeals work in the long-term and that something other than fear is likely also to be elicited. Emotions are complicated, as our results demonstrate.

7.1. Future Research

The current study raises several issues and suggests three primary considerations for future research. *First*, more research is needed in examining threat and coping appraisals separately to better understand how their associated constructs are related to behavioral intentions and changes in behavior, whether modeled using PMT or other theoretical approaches.

Second, fear levels should be measured when fear appeals are used (e.g., [17]), but fear should not be the only emotion measured. The current study suggests that using fear may well lead to higher levels of fear, but also higher levels of other types of negative emotions and reduced levels of positive emotions.

Third, more longitudinal studies are needed to assess the long-term impact of triggering a short-term negative emotion. These studies should examine whether any long-term changes in emotional states have occurred and whether success was achieved with respect to the targeted behavior(s) after a delay of some weeks.

References

[1] K. Renaud and M. Dupuis, "Cyber security fear appeals: Unexpectedly complicated," in *Proceedings of the New Security Paradigms Workshop*, pp. 42–56, 2019.

[2] L. Dodsworth, *A State of Fear*. UK: Pinter & Martin, 2021.

[3] M. Dupuis and K. Renaud, "Scoping the ethical principles of cybersecurity fear appeals," *Ethics and Information Technology*, pp. 1–20, 2020.

[4] V. Zimmermann and K. Renaud, "The nudge puzzle: matching nudge interventions to cybersecurity decisions," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 28, no. 1, pp. 1–45, 2021.

[5] A. M. Isen, "Toward understanding the role of affect in cognition," in *Handbook of Social Cognition* (R. S. Wyer and T. K. Srull, eds.), p. 179–236, L. Erlbaum Associates, 1984.

[6] E. A. Waters, "Feeling good, feeling bad, and feeling at-risk: a review of incidental affect's influence on likelihood estimates of health hazards and life events," *Journal of Risk Research*, vol. 11, p. 569–595, Jul 2008.

[7] D. Watson and L. A. Clark, *The PANAS-X: Manual for the Positive and Negative Affect Schedule - Expanded Form*. University of Iowa, 1994.

[8] D. Watson, L. A. Clark, and A. Tellegen, "Development and validation of brief measures of positive and negative affect: The panas scales," *Journal of Personality and Social Psychology*, vol. 54, pp. 1063–1070, Jun 1988.

[9] J. S. Lerner and D. Keltner, "Beyond valence: Toward a model of emotion-specific influences on judgement and choice," *Cognition & Emotion*, vol. 14, no. 4, p. 473–493, 2000.

[10] G. Loomes and R. Sugden, "Regret theory: An alternative theory of rational choice under uncertainty," *Economic Journal*, vol. 92, p. 805–824, Dec 1982.

[11] G. F. Loewenstein, E. U. Weber, C. K. Hsee, and N. Welch, "Risk as feelings," *Psychological Bulletin*, vol. 127, no. 2, p. 267–286, 2001.

[12] J. P. Dillard, "Rethinking the study of fear appeals: An emotional perspective," *Communication Theory*, vol. 4, no. 4, pp. 295–323, 1994.

[13] F. Mwagwabi, T. J. McGill, and M. Dixon, "Short-term and long-term effects of fear appeals in improving compliance with password guidelines.," *Communications of the Association for Information Systems*, vol. 42, pp. 147–182, Feb 2018.

[14] J. L. Jenkins, M. Grimes, J. G. Proudfoot, and P. B. Lowry, "Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals," *Information Technology for Development*, vol. 20, no. 2, pp. 196–213, 2014.

[15] F. Mwagwabi, T. McGill, and M. Dixon, "Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines," in *47th Hawaii International Conference on System Sciences*, pp. 3188–3197, IEEE, Jan 2014.

[16] A. C. Johnston, M. Warkentin, and M. Siponen, "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly*, vol. 39, pp. 113–134, Mar 2015.

[17] S. Boss, D. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors," *MIS Quarterly (MISQ)*, vol. 39, no. 4, p. 837–864, 2015.

[18] S. Milne, S. Orbell, and P. Sheeran, "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions," *British Journal of Health Psychology*, vol. 7, no. 2, p. 163–184, 2002.

[19] A. Osman, F. X. Barrios, J. R. Osman, R. Schneekloth, and J. A. Troutman, "The pain anxiety symptoms scale: psychometric properties in a community sample," *Journal of Behavioral Medicine*, vol. 17, no. 5, p. 511–522, 1994.

[20] L. M. McCracken, C. Zayfert, and R. T. Gross, "The pain anxiety symptoms scale: development and validation of a scale to measure fear of pain," *Pain*, vol. 50, no. 1, p. 67–73, 1992.

[21] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, no. 4, p. 34–40, 2008.

[22] A. Vance, D. Eargle, K. Ouimet, and D. Straub, "Enhancing password security through interactive fear appeals: A web-based field experiment," in *2013 46th Hawaii International Conference on System Sciences*, p. 2988–2997, Jan 2013.

[23] A. Vance, D. Eargle, D. Straub, and K. Ouimet, "Do security fear appeals work when they interrupt tasks? a multi-method examination of password strength," *MIS Quarterly*, Forthcoming.

[24] J. L. Jenkins, M. Grimes, J. G. Proudfoot, and P. B. Lowry, "Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals," *Information Technology for Development*, vol. 20, p. 196–213, Apr 2014.

[25] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology*, vol. 19, no. 5, p. 469–479, 1983.

[26] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, p. 93–114, 1975.

[27] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," *Psychological Review*, vol. 84, no. 2, p. 191–215, 1977.

[28] S. Milne, P. Sheeran, and S. Orbell, "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *Journal of Applied Social Psychology*, vol. 30, no. 1, p. 106–143, 2000.

[29] R. W. Rogers, "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation," *Social Psychophysiology: A Sourcebook*, p. 153–176, 1983.

[30] V. Zimmermann and N. Gerber, "The password is dead, long live the password–a laboratory study on user perceptions of authentication schemes," *International Journal of Human-Computer Studies*, vol. 133, pp. 26–44, 2020.

[31] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild," *Computers & Security*, vol. 61, p. 130–141, Aug 2016.

[32] M. Dupuis, T. Geiger, M. Slayton, and F. Dewing, "The use and non-use of cybersecurity tools among consumers: Do they want help?," in *Proceedings of The 20th Annual Conference on Information Technology Education (SIGITE '19)*, p. 81–86, ACM, Oct 2019.

[33] R. Crossler, "Protection motivation theory: Understanding determinants to backing up personal data," in *The 43rd Hawaii International Conference on System Sciences (HICSS)*, p. 10, 2010.

[34] M. Dupuis, B. Endicott-Popovsky, and R. Crossler, "An analysis of the use of amazon's mechanical turk for survey research in the cloud," in *International Conference on Cloud Security Management*, Oct 2013.

[35] Z. R. Steelman, B. I. Hammer, and M. Limayem, "Data collection in the digital age: Innovative alternatives to student samples.," *MIS Quarterly*, vol. 38, no. 2, p. 355–378, 2014.

[36] K. Witte, K. A. Cameron, J. K. McKeon, and J. M. Berkowitz, "Predicting risk behaviors: Development and validation of a diagnostic scale.," *Journal of Health Communication*, vol. 1, no. 4, p. 317–341, 1996.

[37] B.-Y. Ng and M. A. Rahim, "A socio-behavioral study of home computer users' intention to practice security," in *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, p. 7–10, 2005.

[38] M. J. Dupuis, R. E. Crossler, and B. Endicott-Popovsky, "Measuring the human factor in information security and privacy," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, p. 3676–3685, IEEE, Jan 2016.

[39] M. P. Keesler and B. Keesler, *Mohawk: Discovering the Valley of the Crystals*. The Keesler Family; Distributed by North Country Books, 2008.

[40] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *Journal of Applied Psychology*, vol. 88, no. 5, p. 879–903, 2003.

[41] J. Hair, W. Black, B. Babin, and R. Anderson, *Multivariate data analysis*. Prentice Hall, 7th ed., 2010.

[42] W. W. Chin, "Commentary: Issues and opinion on structural equation modeling," *MIS Quarterly*, 1998.

[43] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, p. 1–21, 2015.

[44] C. M. Ringle, M. Sarstedt, and D. W. Straub, "A critical look at the use of PLS-SEM in MIS Quarterly," *MIS Quarterly*, vol. 36, no. 1, p. iii–xiv, 2012.

[45] F. A. Masterson and M. Crawford, "The defense motivation system: A theory of avoidance behavior," *Behavioral and Brain Sciences*, vol. 5, no. 4, pp. 661–675, 1982.

[46] C. C. Gill, R. T. Kane, and T. G. Mazzucchelli, "Activation, avoidance, and response-contingent positive reinforcement predict subjective wellbeing," *Journal of Happiness Studies*, vol. 20, no. 2, pp. 331–349, 2019.

[47] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *Journal of Applied Psychology*, vol. 88, no. 5, p. 879–903, 2003.