Cyber Security Fear Appeals: Unexpectedly Complicated

Karen Renaud
University of Abertay, Dundee, UK
Rhodes University, Grahamstown, South Africa
University of South Africa, Pretoria, South Africa
k.renaud@abertay.ac.uk

Marc Dupuis
University of Washington
Bothell, Washington, USA
marcjd@uw.edu

ABSTRACT

Cyber security researchers are starting to experiment with fear appeals, with a wide variety of designs and reported efficaciousness. This makes it hard to derive recommendations for designing and deploying these interventions. We thus reviewed the wider fear appeal literature to arrive at a set of guidelines to assist cyber security researchers. Our review revealed a degree of dissent about whether or not fear appeals are indeed helpful and advisable. Our review also revealed a wide range of fear appeal experimental designs, in both cyber and other domains, which confirms the need for some standardized guidelines to inform practice in this respect. We propose a protocol for carrying out fear appeal experiments, and we review a sample of cyber security fear appeal studies, via this lens, to provide a snapshot of the current state of play. We hope the proposed experimental protocol will prove helpful to those who wish to engage in future cyber security fear appeal research.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; Usability in security and privacy; • **Applied computing** → **Psychology**; **Sociology**.

ACM Reference Format:
Karen Renaud and Marc Dupuis. 2019. Cyber Security Fear Appeals: Unexpectedly Complicated. In *New Security Paradigms Workshop (NSPW '19), September 23–26, 2019, San Carlos, Costa Rica.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3368860.3368864

1 INTRODUCTION

[1] *This is your computer*
This is your computer if it gets hacked
You should take precautions
Any questions?

The citizen of the 21st century has probably been subjected to this kind of message, in essence a cyber security "fear appeal". These messages attempt to scare people into taking a particular recommended action to secure their information and devices.

[1] Inspired by [178]

NSPW '19, September 23–26, 2019, San Carlos, Costa Rica

ACM ISBN 978-1-4503-7647-1/19/09…$15.00
https://doi.org/10.1145/3368860.3368864

The rationale for the use of fear appeals is first, that if you can make people care about something, they are more likely to take the recommended action, and second, that eliciting the fear emotion, by highlighting unpleasant consequences, is likely to make them care.

Why not just tell people what to do? The problem is that knowledge does not reliably convert to behavior [98, 113]. Hence eliciting emotion to prompt action seems worth considering [102, 180], and fear is a powerful emotion.

Fear appeals have been used for decades [23, 58, 61, 133, 159], if not centuries [143]. Proponents of the use of fear appeals [12, 159, 165], consider them efficacious in persuading people to change their behaviors. Others consider the deployment of fear appeals misguided, arguing that the belief in their efficacy to be based on intuition and weak evidence [2, 19, 86, 88, 90, 94].

In cyber security, too, some advocate the use of fear appeals [82, 83, 169] while others consider them counter-productive [95, 109]. Over the past decade, voices have been raised to warn against the use of fear in behavioral interventions [19, 102, 127].

The fact that there is dissent in this domain means that we should not unthinkingly reach for a fear appeal when we are confronted with an ill-advised or absent cyber security behavior. It is important for the deployers of cyber security fear appeals aimed at the general public to base their practices on solid empirical and scientific evidence. Otherwise we risk doing more harm than good.

Consider, for example, the "Scared Straight" program [49]. The idea was that adolescents with behavioral problems would be taken to a jail to meet with inmates, who would "scare" them into abandoning their wayward ways. A movie with that name appeared in 1978, popularizing the scheme. Subsequent studies have now discovered that not only does this program not deliver its promised outcomes, but that it actually has harmful effects [135].

Another example is the "baby doll" scheme, which attempts to put adolescents off teenage pregnancies by making them aware of how hard it is to take care of a new baby. The scheme attempts to make the long-term consequences of a momentary decision more salient. Initial evaluations were positive [131] but a subsequent evaluation, in 2016, found that the program did not achieve what it was meant to achieve. In fact, those who participated were *more* likely to have a teenage pregnancy [112]. These examples serve to demonstrate that strong emotions, while intuitively seeming powerful motivators for behavioral change, can lead to unintended outcomes, and actually backfire.

Some domains report efficaciousness of fear appeals: e.g., health [181] and beauty & personal care [11]. Others report failures: e.g., climate change [48], reckless & drunk driving [101, 110] and HIV/AIDS [45, 120]. We do not know whether cyber security is sufficiently similar to any of these such that we could predict the extent to

which cyber security fear appeals would be likely to succeed, or fail. We need to carry out more well-designed cyber security fear appeal studies before we will be able to draw a conclusion either about the cyber domain as a whole, or particular behaviors within the cyber domain.

It would be beneficial for cyber security fear appeal researchers to have guidelines to inform their studies. In formulating these, we can benefit from the extensive literature on fear appeals in other more mature domains.

We first present an overview of the wider literature on fear appeals (Sections 2 and 3). Section 4 then proposes a model for fear appeal experiments and reviews a range of cyber security fear appeal studies through that lens. Section 5 brings all our insights together to conclude the paper.

2 FEAR APPEALS: STATE OF PLAY

Fear is essentially an emotion, and emotions, both positive and negative, act on humans as follows [38]: emotions arise from the individual's assessment of a situation, have a biological basis, are informed by learning, and unfold over time, while individuals continuously attempt to regulate their emotions.

Fear is invoked when a threat exhibits characteristics as shown in Table 1 (left column). Hence fear appeals, as we see in the next section, often include matching components (right column).

Fear Characteristic	Appeal Content
important	significance and personal relevance
negatively valenced	severity
impending	susceptibility
requiring effort to engage with	response efficacy
it is possible to mitigate	action and self efficacy in carrying it out

Table 1: Characteristics of Fear (left) [38, 130, 178] and the Matching Fear Appeal Communication Intent (right)

Dillard [38] explains that the idea of adding fear to appeals is grounded in the belief that persuasion will follow induced fright; that fear will propel people to take protective action [54]. The target then, according to the theory, will seek to reduce the feelings invoked by the appeal. A specific action is recommended to give them a way to achieve this.

2.1 Fear Appeal Components

Table 1's right hand column suggests what the core components of fear appeals should be, and these components are confirmed by the literature on fear appeals. The components are ordered here as recommended by [39, 97].

A: Details about the importance of the threat (*induce the fear* [97]):

(1) A statement of the *cause* of the threat, emphasizing personal **susceptibility** [165].
(2) A statement about the *consequence* of the threat, emphasizing the **severity** [37, 150, 165].

A fear appeal can provide *implicit* or *explicit* threat information [181]. For example, an implicit appeal could show a picture of a hacker crouched behind a computer screen, and the recipient has to figure out what the hacker is doing. Explicit information shows a hacker taking over webcams and watching people in their living rooms. Implicit appeals are open to misinterpretation.

B: A statement related to **response efficacy** (*action can be taken to mitigate the threat* [39, 102, 168]). Lewis *et al.* [102] highlight the importance of focusing the response efficacy part of the message on *the individual's* role in dealing with the threat.

C: Feasible **recommended actions** (*how to assuage the fear*) [95, 97, 178].

D: A statement related to **self efficacy** (*the individual is able to take the action* [10, 32, 39, 46, 61, 62, 133]). This is important because fear, *combined with high efficacy*, produces the greatest behavioral change, whereas messages conveying low efficacy are likely to trigger maladaptive coping responses such as avoidance or reactance [133, 180]. Dillard *et al.* conclude that "when actions are seen as desirable, people perform those actions *if they are able*" [38, p.1012] (emphasis ours).

2.2 Recommended Action Dimensions

There are three dimensions to the kinds of actions that are recommended during the fear appeal (cyber security examples are provided in Table 2).

The *first* is whether it is a one-off or a repeated action [165]. A polio vaccination is an example of the former, and breast examination an example of the latter.

The *second* dimension is related to the nature of the activity itself [2]: omission (do not do this), commission (do this) or inhibit (beware). Commission activities can be preventative, corrective or detective.

The *third* and final dimension is suggested by Insko *et al.* [77], who make a distinction between initiating a new behavior and changing an existing behavior.

		Frequency	
		One-Off	***Repeated***
Action Type	***Don't***	Use a Specific Privacy-Invasive Smartphone App	Use Public WiFi
	Do	Install a Password Manager	Use a VPN
	Beware	Disposing of Used Storage Media	Email Links and Attachments

Table 2: Cyber Security Recommended Action Dimensions and Cyber Examples

2.3 Interactions

The fear appeal components are not independent. Firstly, *perceived* efficacy (combined response and self efficacy) has to be higher than the *perceived* threat. If people do not feel that the actions they can take will ameliorate the threat, they are likely to choose not to act [181]. Self efficacy also interacts with response efficacy and susceptibility [106]. Two of these need to be high to prompt action. If only one is high, people are likely to engage in maladaptive responses. Moreover, Popova [137] argues that the relationship between severity and susceptibility is multiplicative, i.e., if either is considered unimportant, there is no motivation to act.

2.4 Fear Appeals & Behavior Change

Tengland [166] cites Rosenberg [151], who proposes a teleological scientific model of individual behavioral choices. These are depicted in the steps in Figure 1.

Tengland [166] explains that most behavioral change interventions, as enumerated by Buchanan [21], focus on one or more of these "steps". Security awareness drives focus on (1) and (4), and fear appeals, or what Tengland calls, *"Scare Campaigns"*, attempt to manipulate wants (1 and 4) and provide information about recommended actions (2 and 3). Some will augment messages with information about response efficacy (2 and 3) [39] and self efficacy (5 and 6) [165]. Very few fear appeal behavioral change models acknowledge the notion of opportunity (7).

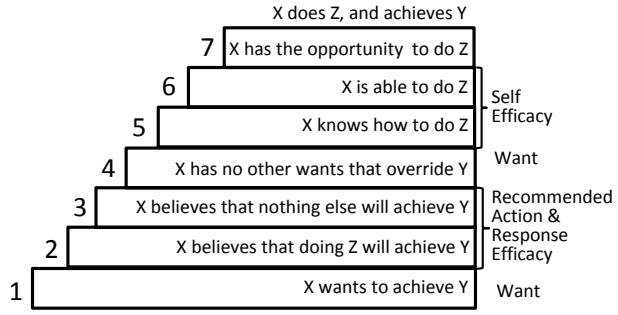

Figure 1: Progression to Taking Recommended Action. X=Person, Y=Secured Device, Z might be Encryption in the Cyber context

Deterrence is different from fear appeals. Fear appeals seek to draw people up the staircase firstly by exciting the fear emotion to propel them, and then scaffolding their progress by providing 2, 3, 5 & 6. Deterrence, on the other hand, occurs when people are dissuaded from wanting to achieve the action, or when they are not convinced of the existence or efficacy of 2-7.

2.5 A Selective Review of Fear Appeal Behavioral Change Models

One of the first theories to explain responses to fear appeals is *Fear as Drive* [74]. The rationale behind this theory is that fear induces a feeling of unpleasantness, which the recipient will act to resolve or reduce [38, 78, 114, 117].

This theory was criticized by Leventhal [97], who argued firstly that the model assumes that fear is a mediator of acceptance of the message. The drive theory also treats fear as a unitary concept, whereas Leventhal argues that fear is more nuanced than this. Leventhal also says that this model is somewhat simplistic, because it suggests that the severity of the threat and the resulting intensity of the fear is more likely to persuade people to take preventive action. Yet some people undeniably respond to fear appeals by avoiding the issue or denying the threat.

The next model is the *Parallel Response Model*, which does not require emotional arousal as a necessary pre-condition to preventive or adaptive behavior. This model considers fear appeals to trigger two independent processes: fear control and danger control [97], the second of which is a problem solving process [38]. In this model, fear and danger control processes may interact but are essentially independent. If the person seeks purely to control the fear, they might do this by avoidance or denial, and this might well deter danger control processes (preventive actions) from being activated — the fact that all the cognitive processes are involved in fear control essentially lead to persuasion resistance.

Rogers [148] proposed *Protection Motivation Theory (PMT)*, which focuses primarily on the danger control branch of the parallel response model. This model has four components: (1) perceived vulnerability, (2) perceived severity, (3) response efficacy and (4) self efficacy. The first two constitute the threat appraisal and the second two the coping appraisal. Dillard [38] argues that this model *cognitivizes* passion into protection motivation.

Witte [178] proposed the *Extended Parallel Process Model* (EPPM) to address three perceived issues with the field of fear appeal research. In particular: (1) the conflating of threat and fear, (2) a focus on message acceptance and neglect, with no in-depth focus on *why* such messages fail, (3) that the role of threat and self efficacy are recognized as important, but the means by which they exert their influence is not well understood. This model builds on the fear-as-drive [78], protection motivation [148] and parallel response models [97]. In essence, Witte thereby proposes putting fear back into fear appeals.

This model suggests that fear appeals trigger two kinds of appraisal, the *first* being an appraisal of the threat. This appraisal will decide whether the threat is moderate or high, and fear may result. The *second* appraisal is an assessment of the efficacy of a response. If the assessment of both are high, a danger control process will be initiated, and the recipient is likely to take the recommended action. The fear control process is initiated when the message recipient believes that it is not possible to mitigate the threat, and, in this case, the fear emotion might trigger a maladaptive response.

3 UNRESOLVED ISSUES

Fear has been used in a number of areas to influence human behavior, either to persuade people to cease or reduce particular negative behaviors, or initiate beneficial behaviors [12, 159, 165].

Yet there are those who believe that fear appeals are contra-indicated [19, 86, 88, 90, 94]. Kok *et al.* [88] refer to "the false belief" in fear appeals in his denunciation, concluding that risk perception is not a reliable determinant of behavior. French *et al.* [53] report that their analysis of systematic reviews of fear appeals revealed very little evidence that risk information impacted health behaviors. Peters *et al.* [134] call fear "a bad counselor". Here, we explore specific differences of opinion.

3.1 Viability & Advisability

3.1.1 Fear as Motivator. It has been argued that the inclusion of fear in an appeal will improve the persuasiveness of messages [41, 165], increase engagement [141], enhance information processing [119] and render the message memorable [16].

Ruiter *et al.* [152], on the other hand, report that although fear does indeed impact attitude and intention, this does not necessarily convert into actual behavior. They argue that fear could arouse defensive reactions [171] (evidenced by [105]) and bias in information processing, which could result in ineffective or no behavioral

change. Indeed, researchers warn that fear levels are *inversely* associated with persuasiveness [24, 160].

Floyd *et al.* [50] conclude, from their meta-analysis of fear appeals, that perceived self-efficacy is far more influential than fear. This is confirmed by [118, 129]. O'Neill and Nicholson-Cole [127] argue that fear appeals actually do not have much potential for encouraging genuine engagement, in their case with climate change communications.

Yzer *et al.* [183] point out the difficulty of pinning down the actual role of the fear part of fear appeals. They cite Earl and Albarracín [45] to point out that studies have not yet provided compelling evidence for a link between fear appeal construction and message acceptance.

3.1.2 How Fear is Processed. There is evidence that indicates that phishing messages work because they elicit fear, and this makes people likely to act without deliberation [173]. This suggests that phishing messages that induce fear cause the usual cognitive processing to be bypassed. Given that this is so, can we expect a well-intended fear appeal to be processed cognitively and thoughtfully? Some authors argue that when perceived efficacy is high, the fear appeal is more likely to be cognitively processed [133, 137]. Does this mean that those with high self efficacy effectively experience a lower level of fear because they know how to cope with the threat? If people *do* experience real fear, would they perhaps carry out the recommended action in the heat of the moment to assuage the emotion, and then abandon it once the fear has worn off? The unanswered and important question is whether fear is indeed effective in motivating long-term adoption of advised behaviors.

3.1.3 Cues and Rewards. Because many cyber security behaviors need to be repeated, it would be beneficial if these behaviors became habitual. Duhigg [42] explains that habits are cued by something in the environment, and that the person gains some kind of reward from carrying out the behavior. Consider the fear appeal — if this is used, is the idea to elicit fear as a cue every time the behavior needs to be carried out? Moreover, what is the reward? Is it assuaged fear? This is surely unsustainable and undesirable.

3.1.4 Ethics. Fear appeals might be considered to violate autonomy [166], restrict choice [116], cause psychological harm [63, 76], demonize those who behave insecurely [182] or have negative impacts on long-term security behaviors.

Negative emotions can have long-term health consequences [29], and the cumulative effect of appeals across the spectrum of domains is likely to be significant. The question is whether fear appeals are warranted to address the full range of insecure behaviors. Moreover, if we *do* demonstrate the efficacy of fear appeals, they may start to be used extensively, and the cumulative and potentially negative impact is likely to become even more significant.

Demonization is another consideration in the use of fear appeals. By targeting specific groups believed to need the change in the behavior the most, it may result in causing them harm through this demonization. For example, as the AIDS crisis began to unfold, gay individuals were targeted with specific messaging via fear appeals to help prevent the spread of HIV. However, this also led to the reinforcement of negative stereotypes and the demonization of gay people as a group [182]. Beyond the demonization of the target group, a fear appeal aimed at a specific group may result in complacency in those not targeted [64]. They may believe that since they were not mentioned specifically, they are not at risk. Indeed, one of the very first papers in the human-centered security research field makes this very argument [1], that people who behave insecurely are blamed for this, instead of organizations considering that their demands are unreasonable.

Albarracín *et al.* [2] argue that even if fear appeals do not work, they will not do harm. The two examples that we mentioned in the introduction appear to contradict this, as do [96, 140]. Yet there is a dearth of field studies into the long term impacts of fear appeals across most domains [183]. This means that we do not have enough evidence, just now, to come to an evidence-based conclusion about the harm that could be caused by use, or overuse, of this behavioral intervention in the cyber security domain.

The general approach taken by utilitarian theorists [116] is to assess whether the benefits of an action outweigh the costs. This is especially true in the United States where research is often conducted under the philosophical umbrella of utilitarian ethics [59]. Based on this approach, as long as the benefit derived from a fear appeal is greater than the costs, then the use of fear appeals is ethical. This benefit does not need to be with the target of the fear appeal. Instead, it is the net benefit to society as a whole with consideration given to any associated costs, whether to the target of the fear appeal or another entity, such as those that may become complacent in performing the desired behavior if they are not the target of the fear appeal. This net benefit may be positive in some circumstances. However, as we just noted it is not always possible to make this assessment since the benefits that are derived from fear appeals is not entirely clear, with contradictory evidence abounding.

For example, a fear appeal could be designed with the goal of reducing the spread of ransomware. The target of the fear appeal might be Windows users. Some of the recipients of the fear appeal may become upset at the prospect of losing all of their information and, instead of performing a recommended action, they instead choose to do nothing. They may even experience a certain level of psychological harm. Likewise, Apple users may see the targeted fear appeal and become complacent, thinking that since they were not the target of the fear appeal they must be invulnerable. This complacency may result in some Apple users having their devices infected by ransomware, along with the Windows users who decided against performing the recommended action. Likewise, some individuals may become upset and experience a certain level of psychological harm from being targeted by the fear appeal.

While all of this would be unfortunate, so long as the fear appeal campaign was beneficial to society as a whole then it would be considered ethical by deployers that use a utilitarian ethical framework, despite the inherent imperfection. Thus, the failures would not be discounted or otherwise ignored, but instead compared to all of the benefits provided by the fear appeal. Ultimately, is the overall decrease in successful ransomware attacks worth the cost of designing and deploying the fear appeal, the possible increase in ransomware attacks among some, as well as the possible psychological harm inflicted on a few of those targeted by the fear appeal?

3.1.5 Threats Warranting Fear Appeals. There is very little notion of the kinds of threats that warrant the use of fear-based interventions [93]. So, for example, should we use fear to motivate people to make backups, to use a VPN, or to encrypt their hard drives? What about less widespread precautions, such as covering web cams or eschewing Social Networking websites? At the moment, it seems as if deployers arbitrarily decide that fear appeals are appropriate and warranted in their context.

What is required is an objective way of judging whether or not the use of fear is indicated, especially given the ethical concerns mentioned in the previous section. Without some kind of criterion, it is something of a free-for-all at the moment.

3.1.6 Noise. Any fear appeal experiment has to confront potential confounds:

Fear Appeal Fatigue: Many domains deploy fear appeals and the appeal enters a noisy environment to compete for attention. People might suffer from "fear appeal fatigue" [20]. Simpson also points out that there is evidence of growing resistance to some kinds of fear appeals among the general public [157], perhaps evidence of what MacCurdy [105] refers to as *being afraid of being afraid.*

Other Influences: It is difficult to isolate the impact of a fear appeal used in a single study within a noisy environment. Consider smoking, for example. Cigarette packets display fear appeals in many countries, doctors generally confront people with the dangers of smoking, and people are offered smoking cessation advice at pharmacies. If a person is targeted by a new smoking-related fear appeal and stops smoking, can we realistically attribute this purely to the latest appeal?

Second-Order Effects: It is hard to know how well experimental findings that are based on individual responses to fear appeals will transfer to widespread public campaigns, where the communication is competing with a myriad number of other communications. In particular, we do not know what will happen if and when people start to discuss the topic [69]. Such dispersion of impact is hard to measure or assess because it occurs dynamically and unpredictably in the wild.

3.1.7 Recommended Action. There are a number of findings to be considered that apply to the different kinds of recommended actions.

Action Frequency: Tannenbaum *et al.* [165] report that fear appeals worked better for one-off behaviors than for repeated behaviors. Success, however, is related to whether recipients embrace the cause and adopt long-term behavioral changes. In cyber security, encrypting your mobile phone is a one-off behavior, and making backups is a repeated and ongoing behavior. If a fear appeal induces someone to make one backup, but not to do this regularly, this is of limited use.

Action Type: Tannenbaum *et al.* [165] report that fear appeals were more likely to prompt people to engage in detection behaviors than in preventative behaviors. Floyd [50] reported that cessation behaviors were more likely to be carried out in response to a fear appeal than initiation of new behaviors. Hence all recommended actions are not equal in this domain.

New or Pre-Existing Actions: Insko *et al.* [77] argue that if the recommended action has to do with changing the way people are currently acting, they are more likely to reject the message. This could be because, as Ariely and Norton [6] argue, previous behaviors create preferences. This might also be a manifestation of the endowment effect related to pre-existing routines [144]. If engaging with a particular security-related behavior has been a negative experience, it becomes much harder for a future related fear appeal to be efficacious [170].

Feasibility: Ruiter *et al.* [152] argue that the provision of specific action instructions is essential, because, without this, fear appeals are likely to fail to change behavior. Insko *et al.* [77] suggest that the failure of many fear campaigns could be attributed to the fact that the message does not provide the hearer with *believable* information about how the fear can be assuaged. This is confirmed by a study of actual fear appeals in Sweden [4].

3.2 Experiments

3.2.1 Acceptance. The recipient of a fear appeal might reject the appeal because they believe that the consequence does not apply to them, but only to others [15]. They might also reject the appeal because accepting it would require them to change their beliefs, mandate action that they are unwilling to take or because they do not like the emotion the appeal is eliciting [164]. They may also believe that the consequence has been exaggerated and that the message source is not credible, or the claims unrealistic [104]. They might reject the import of the message if it is not believable [67, 70, 92, 160].

If they *do* accept the message, they might deal with the negative emotions triggered by fear appeals by engaging in fear control: denying the reality of the threat, or the negativity of the consequences [15, 153], as suggested by the EPPM. If they do engage in danger control, they could also decide not to act because the recommended action itself seems abhorrent or unappealing [32, 158]. Leventhal and Watts [99] found that their participants chose not to take the recommended action because it might detect a disease and they dreaded the consequent treatment [115]. When acceptance tests are used in experiments, they ought to explore reasons for non-acceptance as well reasons for post-acceptance inaction.

3.2.2 Elicited Fear Levels. Fear appeals can be designed to elicit low, moderate or high fear. What does the literature say about the advisability of different levels?

In 1953, Janis and Feshbach published a seminal paper titled "Effects of fear-arousing communications" [78]. They reported that: "*The over-all effectiveness of a persuasive communication will tend to be reduced by the use of a strong fear appeal, if it evokes a high degree of emotional tension without adequately satisfying the need for reassurance*" (p.92). Many papers cite this one to warn against the use of fear appeals that will lead to high levels of fear [14, 24]. In warning against the use of high fear in fear appeals, researchers explain that fear levels are inversely associated with persuasiveness [24, 160], or backfire altogether by failing to induce behavioral change [78]. Krisher *et al.* [90] also argue that strong fear appeals can trigger maladaptive responses. Rhodes [145], on the other hand, finds that eliciting moderate levels of fear worked better than either low or high levels in their study related to driving speed.

Other researchers feel that a reluctance to elicit high fear in fear appeals is misguided, and neutralizes the potential power of a fear-based appeal. Hill *et al.* [68] ran a high-fear 'stop smoking'

campaign and reported that the campaign had a high impact, with people taking steps towards ceasing smoking. Leventhal *et al.* [98] discovered that a high fear condition motivated participants to form strong intentions to act and Leventhal *et al.* [100] demonstrated that both high and low fear appeals could lead to actual reductions in smoking. Other studies also report on the efficaciousness of high fear [46, 62] although these studies often measured attitude and behavioral intention rather than actual behavior.

The advocates of high fear in appeals essentially consider fear appeals to fit into a variance theory of human behavioral change [37, 111]. The variance theory assumes that particular factors are necessary and sufficient conditions for prompting a particular behavior, with greater magnitude of the triggering factor making the outcome more likely.

It is worth mentioning that other researchers consider human behavioral change something that can be modeled by a stage model such as process theory [33]. For example, Cho and Salmon [26] argue that people would be less receptive to fear appeals if they were in a pre-contemplative state of mind, than if they were ready to make a change. Cho [25] concludes that fear appeals are most likely to fail in those who need them most, and that they are the ones most likely to engage in fear control responses. De Hoog *et al.* [37] cite [33] explain that the stage model approach considers that people can be brought to a defensive state of mind, which motivates them to act, as long as the actions themselves are deemed to be efficacious. If this is so, greater attention to the feasibility of the recommended action, both in terms of response efficacy [163] and the individual's self efficacy [153], and focusing on presenting feasible solutions [108] is warranted when designing fear appeals, rather than fixating on levels of fear to be elicited.

3.2.3 Delay Before Action. While people might indeed experience fear immediately post-message, and intend to do something to assuage it, this feeling might not endure. Janis and Feshbach [78] argue that people might be more willing to act if such action is immediately feasible. If there is a significant delay between the fear appeal and the opportunity to act, the effect of the fear appeal might wear off. Leventhal and Watts [99] found evidence that a delay between the appeal and the opportunity to act made action less likely. Leventhal [97] argues that a delay might play a role towards triggering fear control actions. Leventhal and Watts explain that positive emotions are far more enduring, and recommend focusing on eliciting these rather than on triggering negative emotions such as fear.

3.2.4 Measurement.

Different Outcomes: There is a wide variety of practice in this area, some measuring *attitude* post-appeal [106, 156], *attitude & behavioral intention* [145], *attitude & behavior* [84] or *attitude, intention & behavioral outcomes* [32, 142]. With respect to behavior, some rely on self report [89] while others measure actual behavioral outcomes [142]. This makes it difficult to compare the efficacy of fear appeals across different studies. It would be beneficial to have a recommended experimental design protocol so that future studies can be compared.

Measuring Fear: The measurement of fear in fear appeal studies is variable and often considered inadequate [88]. As such, O'Keefe [124] reports that fear appeals, in general, have not yet been proven to induce high levels of fear. Yzer *et al.* [183] point out that most studies of fear appeals rely on self report of positive vs. negative affect [145]. This might not be the best way to measure fear intensity or valence. Boster and Mongeau [18] reviewed a number of fear appeal studies and discovered that authors generally did not report the reliability of the fear measure instrument they used. They also argue that the use of one-item measures of perceived fear is insufficient.

Action Frequency: When it comes to a repeated and ongoing recommended action, it is important to distinguish between an initial first attempt and a long-term adoption of action when judging success. Sometimes studies report on success based on one preventative action [7]. In these cases, measuring behavior once, after the first attempt to act on the fear appeal has been taken, could fail to detect a subsequent abandonment of the behavior or a change in attitude [102] (This is likely, given the discussion in Section 3.1.2). This makes it possible for experimenters erroneously to conclude that their fear appeal has delivered the anticipated positive behavioral outcome.

Behavior: In some domains, it is infeasible to measure actual behavior. For example, one cannot monitor the actual use of condoms [2]. In the cyber security field, some behaviors are easy to monitor, such as the installation of a password manager. However, to conclude that an appeal has been successful, there ought to be behavioral monitoring of long-term use of the password manager.

3.2.5 Operationalizing Findings. There is evidence that whether a participant volunteers for a fear experiment, or not, is a strong moderator of the extent to which there will be a correlation between fear levels and resulting attitude [71–73]. Davis and Jansen [34] found that a pre-existing sense of self efficacy, with respect to a particular threat, had a positive effect on attitude towards adopting recommended actions. It might be that volunteers are more capable of mitigating a particular threat than those who do not volunteer, and this would skew outcomes. On the other hand, ethics review boards require researchers to gain informed consent from participants, which reflects willingness, if not direct volunteering. That being so, it is not obvious how an experimenter could rigorously determine how a seemingly efficacious fear appeal would impact unwilling non-volunteers when rolled out to the general public.

Finally, because very few field tests of fear appeals have been carried out [133, 183] we still do not know how well lab- and survey-based findings will apply in the wild.

3.3 Fear Appeal Behavioral Change Models

The models reviewed in Section 2.5 can be criticized in a number of ways.

3.3.1 Starting Points: The models commence at the point where the recipient is issued with the fear appeal. As such, they do not consider a number of pre-existing potential confounds.

Prior Experience: It is unrealistic not to include the prior experience of dealing with the threat presented within the fear appeal [97]. For example, Vaniea *et al.* [170] found that a negative experience of updating an operating system had an impact on future security behaviors.

Existing Practice: O'Keefe [126] used a public communication to persuade people to stop smoking. He reports that the message was accepted by non-smokers but not by smokers, the intended targets.

This suggests that pre-existing practices, and presumably prior decisions to smoke or refrain from smoking, led people either to accept or reject the message. Leventhal [97] review a number of studies showing that vulnerable people (e.g., smokers) were less amenable to fear appeals than invulnerable people [80, 85, 99].

Pre-Existing Knowledge: The models also do not incorporate differences in participants' knowledge. The EPPM model does include individual differences but these seem to feed only into a decision not to respond. Individual differences could also feed into people taking action. For example, one of the authors of this paper routinely covers their PC's webcam — no fear appeal was required; the decision was made based purely on their personal cyber security value system, an influential factor suggested by [152].

Pre-Existing Emotional State: The models do not consider pre-existing emotional state, which is indeed influential [56, 80]. If a person is generally an anxious person, a fear appeal could trigger a fear control response, not because they lack self efficacy, but because of their existing emotional state.

3.3.2 Triggering Other Emotions. Halkjelsvik and Rise [60] combined fear and disgust in fear appeals, but did not observe any greater efficacy of appeals. Lewis *et al.* [103] suggest that, instead of fear, more positive emotional appeals ought to be considered.

3.3.3 Opportunity: Figure 1 incorporates a seventh and final step towards action: that the person has the opportunity to take the recommended action. This is not realistically incorporated into the models [166]. In HIV prevention fear appeals, opportunity is related to availability of condoms [2]. In cyber security, the best way to prevent dragnet surveillance is by using a VPN. The recipient of a snooping-related fear appeal could know this, know exactly how to use a VPN, but not do so. They might not be able to afford the software, or their device might not have enough memory to accommodate the app, or they may live in a country where the use of a VPN is not permitted or considered a revolutionary act.

3.3.4 Feedback: Many of the models fail to include a feedback mechanism. EPPM does include feedback [178] but this seems to feed into fear and not danger control, which is where it is needed to reinforce behavior [52]. In the cyber security domain, it is essential that people are able to judge the response efficacy of the action they take, so that they are motivated to continue the behavior.

3.3.5 Longitudinal Impact: The fear appeal models reviewed in Section 2.5 do not incorporate any notion of realistic long-term measurement, or delay before measurement. The two fear appeal examples mentioned in the introduction seemed efficacious when first evaluated (straight after the appeal) but a retrospective analysis revealed the actual negative outcomes. Hastings *et al.* [63] found that recent studies into the use of fear appeals are reporting much smaller effects than those previously published. This could be because many older studies judged efficacy by measuring intention immediately after message receipt, which is unrealistic in terms of measuring genuine efficacy [102]. Terblanche-Smit and Terblanche [167] found that the long-term efficacy of fear appeals depended on the level of fear, something that was only detected because they measured impact after a delay. The models ideally ought to show that long-term outcomes of a threat requiring repeated behaviors are the real tests of the efficacy of a fear appeal, not the immediate self-reported post-appeal attitudinal, intention-based or one-off behavioral response.

3.3.6 Social Aspects: Bandura [9] mentions a number of key components of fear appeals. One of these is the social support required to support change. The impact of social norms is included in many technology adoption models [75]. It is possible that technology adoption and precautionary action adoption share this feature. Hill *et al.* [68] also mention that some recommended behaviors require long-term support and resources to sustain. It is likely that social support is particularly important when it comes to enduring behavioral change.

3.4 Summary

This section has sought to highlight the areas where researchers diverge in terms of good practice related to deciding whether and how to use a fear appeal (Section 3.1), how to experiment with fear appeals (Section 3.2), and also points out problems related to the behavioral change models reviewed in Section 2.5 (Section 3.3). We now consider the cyber security fear appeal domain.

4 CYBER SECURITY STUDIES

In this section, we will consider fear appeal studies in cyber security. We first bring together the insights from the review to propose an experiment protocol for fear appeals.

4.1 Fear Appeal Experiment Guidelines

Boster and Mongeau [18] argue that the differences in fear appeal outcomes are due to methodological artifacts. Our review of the studies of fear appeals in cyber security exhibits a wide variation in experimental design. We probably need more studies carried out before we can decide whether or not fear appeals are appropriate for use in the cyber security domain.

The gold standard of scientific research is a randomized controlled design where different interventions are delivered to groups in which participants are randomly assigned. This makes it possible to draw comparisons and prove impact [88]. It is also good practice to always have a control group that does not receive any intervention. By randomly allocating participants to different groups, the role of fear in the intervention can be isolated.

4.1.1 Deciding to Deploy. Before deciding, we first have to give due consideration to whether the particular threat warrants the use of a fear appeal (Section 3.1.5), and whether there is sufficient evidence from domains similar to cyber security to suggest that they might be effective. The ethics of the intervention also have to be considered very carefully before proceeding (Section 3.1.4).

4.1.2 Design. Boster and Mongeau [18] suggest a model for a fear appeal experiment, which we have extended in Figure 2.

The fear appeal itself is constructed as recommended in Section 2.1. We have extended this with the following measurement recommendations:

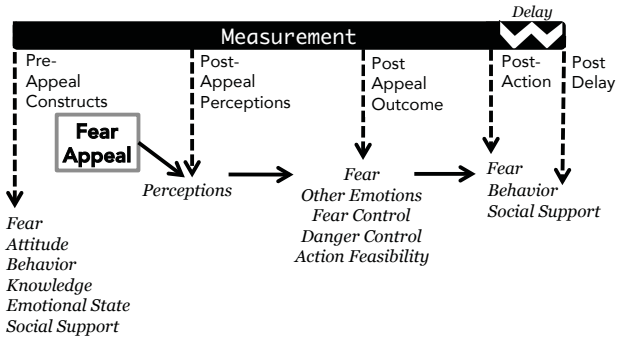

Figure 2: Experiment Model (Extended from [18])

Pre-Appeal measure of: fear [18, 39], emotional state (including anxiety) [18], pre-existing knowledge [123], attitude, behaviors & experiences of dealing with threat [137], demographics [18] and social support [9].

Post-Appeal measures of:

(1) perceived: (1) fear (Section 3.2.2 [38]), (2) self-efficacy, (3) response efficacy, (4) severity and (5) *individual* susceptibility [137, 146]. Perceived severity should be measured on a scale from 0 to 10 and perceived susceptibility from 0% to 100% [177]. Measure other emotions that could have been triggered by the appeal (Section 3.3.2);

(2) feasibility of recommended action(s) [18, 108, 163], which includes measures of *opportunity* to carry it out (Section 3.3.3);

(3) danger control responses (attitude, intentions and immediate behavior [35, 97]). Crossler *et al.* [31] argue that it is better to study actual behaviors than to rely on self-report as gathered by surveys, citing a number of studies to substantiate this claim [5, 107, 162, 174]. *fear control* responses (avoidance, denial, reactance, helplessness and wishful thinking [147, 178]).

Post-Action: fear (to check whether it has been assuaged by the action [38]), and social support [9] to see whether this factor influences success.

Post-Delay: after a period of time: has the person continued with the recommended behavior?

4.1.3 Measuring Fear: It is important to measure fear rigorously. Yzer *et al.* points to emerging research by [85, 128] into more accurate ways of measuring fear. However, Mewborn and Rogers [150] found that self-reported levels of fear and physiological measures of fear were correlated. This means that self-report measures might be a reasonable way of measuring elicited fear in fear appeal studies [137], which would make in-the-wild fear appeal studies more feasible.

4.1.4 Rigor: Boster and Mongeau [18] urge experimenters to use multiple measures for each construct, to ensure maximum reliability. They provide some examples where, even for behavior, multiple measures are possible.

4.1.5 Analysis. Peters *et al.* [132] explain that the analysis should make it possible to report the effectiveness of the individual components of fear appeals, not merely a single behavioral change measure. Moreover, researchers ought to commence with lab studies to test their experimental design, and then proceed to field tests to ensure the veracity of their intervention [183]. Effect sizes should be reported for individual components of the message, and the intervention overall [125].

Analysis should include manipulation checks, to test for confounding factors — credibility of the message (personal susceptibility, perceived severity), or whether other emotions, such as anger, have been triggered by the communication [97].

4.2 Cyber Security Fear Appeal Studies

A sample of cyber security studies that use fear appeals is presented in Table 4. (A few studies that did not employ a fear appeal, but nonetheless did measure the constructs from Protection Motivation Theory, are presented for context.) The included studies are meant to be representative rather than exhaustive of cyber security studies that have employed fear appeals. Particular attention was given to studies appearing in top tier journals or conferences, those that have been cited multiple times, and/or those that represent a different perspective when compared to the other included studies. There are several observations worth noting.

4.2.1 Lack of Pre-Testing. The sample suggests that it is rare for a fear appeal study to measure attitude, behavior, or existing levels of fear (or other affect attributes) prior to the appeal being delivered. While control groups have been implemented on a regular basis and can assess these measures without the effect of a treatment, this does not provide the same level of confidence in treatment effects that a pre-test yields [22]. As a more extreme example, one approach may include a treatment group with a pre-test, one without a pre-test, and a control group to match each of these treatment groups (e.g., [13]). However, experimental designs that incorporate increasingly rigorous methods to control for various factors pose their own set of challenges, such as acquiring a large enough sample size to provide sufficient statistical power [28, 139]. The presence of such challenges, as significant as they may be, do not assuage the need for greater consideration to be given to such approaches.

4.2.2 Fear is Rarely Measured. More than half of the studies do not measure fear. While a fear appeal presumably elicits fear, this assumption is not supported by empirical evidence in a majority of cases and some evidence suggests it does not [175]. Similarly, other types of affect are measured even less often. When a fear appeal is used, it may elicit fear, but it may also elicit other affective states, such as anxiety or hostility [179]. To the extent that fear appeals do increase fear, this may not be occurring in isolation; other affective states may also be increasing or decreasing in their respective levels. Having *a priori* information on an individual's affect unrelated to the fear appeal (i.e., incidental affect), may help researchers better estimate the extent to which the appeal itself contributed to a specific affective state (i.e., integral affect) [55, 172]. From a measurement standpoint, this does pose some challenges since instruments used to measure affect's lower order dimensions can consist of up to 60 items [65, 176]. Perhaps this is another reason (in addition to those that we will discuss shortly) to consider greater deployment of longitudinal studies when using fear appeals.

4.2.3 Recommended Action Procedures are Lacking. Most studies did provide detailed information on the recommended action to be taken to address the threat conveyed via the fear appeal. However, several of the studies did not provide specific guidance on how to effectively carry out the recommended action, such as the specific procedures involved. Watching a video demonstration of how to perform a specific task may provide users with something akin to a vicarious experience and result in higher levels of self-efficacy [8]. Engaging users in actually performing the task would likely have an even stronger effect on self-efficacy through performance accomplishments [8]. Likewise, there is a general lack of assessment on whether participants believe the recommended action is even feasible. They may believe they can perform the recommended action (i.e., self-efficacy), and that the recommended action would be effective (i.e., response efficacy), but it does not mean they believe the recommended action is actually feasible in their individual context [95, 97, 178].

4.2.4 Fear Control is Rarely Assessed. Many of the reviewed studies measure danger control via behavior (observed or self-reported), behavioral intention, or attitude. However, few measure fear control via maladaptive rewards or costs. This may be due to the dominant role Protection Motivation Theory has had in the fear appeal literature since its original formulation and the focus on danger rather than fear control mechanisms [97, 149, 178]. As two separate processes [97], a fear appeal could presumably trigger varying levels of a danger *and* fear control processes. Thus, beyond whether or not a danger control process has been successfully initiated as a result of the fear appeal, it should be of equal interest to determine whether a fear control process has been triggered.

4.2.5 Longitudinal Studies are Needed but Lacking. The majority of the studies occur as a snapshot in time for the participants. They are presented with a fear appeal and then asked to answer some questions and/or their behavior observed. The goal of a fear appeal is to have individuals change their behavior by adopting a recommended action as part of a long-term danger control process. There is no way to know if the fear appeal was successful, unless this adoption is assessed at some later point in time by checking whether the behavior is still occurring. Does adoption actually occur if the desired behavior fails to persist beyond the study? A one-week period seems to be a good starting point for determining whether some level of adoption has been reached after the initial fear appeal (e.g., [3]).

4.2.6 Triangulation. Triangulation is generally not used in fear appeal studies, including in the assessment of affective states (e.g., fear), or the target behavior itself. For example, physiological measures could be used more to confirm self-reports of affective states. While some research has used such measures (e.g., [128, 175]), there has been a general shift away from the physiological aspects of fear and other affective components [154]. Likewise, the studies we reviewed generally detected a positive effect of the fear appeals, but they mostly focused on behavioral *intention*, and detected these via surveys. When they did record behavior, they generally used self-report, which is only a proxy for actual behavior.

5 REPRISE

This review of fear appeals, both in cyber and in other domains, serves to highlight the complexity of this intervention. There is indeed evidence that fear appeals have been successful, but the arguments against their use, and the wide variety of experimental designs and evaluations, make it very difficult to have confidence that they will prove efficacious in encouraging long-term secure behaviors.

5.1 Fear Appeal Context

Table 3 provides examples of contexts within which fear appeals could be used in cyber security, classified in terms of action type (do, don't, beware) from Table 2, and information security's CIA (confidentiality, integrity, and availability) principles. The final row in the table names a consequence that could be used to elicit fear in the fear appeal recipient: something that they probably wouldn't want to happen to them.

	Information Security Principles		
	Confidentiality	***Integrity***	***Availability***
Don't	Use Default Passwords	Use Public WiFi	Share Passwords
Do	Encrypt	Patch Software	Make Backups
Beware	App Permissions	Clicking on Links in Emails	Share Devices
Undesirable Consequence	Identity Theft	Misinformed Decisions	Loss of Productivity

Table 3: Context of Fear Appeal Usage

This table contains the kinds of advice that could be provided as a recommended action within a fear appeal. The fear could be induced by pointing out that the confidentiality, integrity or availability of information could be compromised, and going deeper into how a malicious person could violate this property.

Yet this table is essentially context-independent in terms of the fear appeal recipient. It does not acknowledge that the recipient of the fear appeal is an emotional human being. It is likely that he or she receives the cyber security fear appeal *in addition to* a number of other fear appeals they are being targeted by. The table also does not account for the personal life experiences, access to informal technical support in performing desired behaviors [136], personality differences and mental health states of the recipients. All of these will impact their response to the fear appeal.

Another context consideration is how new or old the desired behavior is to the individual, as well as what the deployer of the fear appeal is asking of that individual. Is the individual being asked to perform a behavior one time, for a specific duration, or is a permanent change being sought? These considerations are advocated by Fogg and Hreha [51] but their behavior grid also incorporates other aspects, such as the familiarity of the behavior to the individual. Once the target behaviors have been classified using their behavior grid, a *Behavior Wizard* is employed to fix on the best behavioral change technique to deploy. In deploying a

fear appeal, these are important considerations because the results of such an analysis may vary considerably from one individual to another.

If cyber security researchers want to experiment with, and deploy, fear appeals, we have to be sensitive to individual differences, and mindful of the damage fear appeals could unwittingly wreak on those who are vulnerable or less able to act to assuage the fear. That this is going to be challenging is obvious. If we want to make use of fear appeals in cyber security, we cannot afford to ignore these realities, which have to be acknowledged in fear appeal design and experimentation.

5.2 Wider use of Fear Appeals

Fear appeals have been studied extensively through laboratory experimentation, understandably so. These types of experiments, after all, do provide the most robust method to determine the extent to which fear appeals may effectuate change, if any. However, as discussed in this paper, greater rigor is needed in designing cyber security fear appeal experiments.

Nonetheless, there is reason to believe that such experimentation is inadequate to fully understand and embrace how cyber security fear appeals are used in the wild, even when such experimentation does have significant rigor. Yet there are opportunities for more ecologically-valid trials. Organizations have been using fear appeals to induce behavioral change as it relates to cyber security policy compliance. We should examine these natural experiments for clues as to their efficacy in real-world settings. For example, several years ago the United States government was disseminating a variety of *cyber doom* scenarios [95]. While this effort was not proven to be successful, and the organization here is arguably the United States as a whole, it does point to some broader challenges.

For example, contrived experiments may lack the realism that is required in security and privacy research [91]. A challenge with realism is that it may raise even more ethical questions. As a consequence, researchers may choose to advocate for greater internal validity at the expense of external validity [91].

Field experiments (e.g., [17]) may help bridge this gap between the controlled confines of a laboratory experiment and less well-controlled organizational settings. While field experiments may address some of the issues raised here, such as finding a better balance between internal and external validity, they nonetheless remain aimed at individual users. That being so, they cannot help us to determine their effectiveness in creating desired change among groups, which is sought in organizational settings.

Moreover, it will remain difficult to understand and consider the many nuances of non-compliance within an organizational setting, including both malicious and non-malicious insider behaviors [44]. Individuals may be non-compliant due either to mistakes (i.e., the non-malicious insider) or other underlying nefarious motives (i.e., the malicious insider). Thus, the fear appeal may have been effective in inducing fear and providing information on how to assuage that fear, but that will not always be enough to combat non-compliance. This would likely be observed more accurately in the wild via natural experiments than either in the laboratory or during field experiments.

Finally, we must also consider the long-term consequences of using fear appeals, both for those being targeted and those that are not. Consider a natural experiment that uses a fear appeal in which a celebrity scares people into believing negative outcomes associated with vaccinations are significantly disproportionate to the actual risks involved [57]. The targeted group in this particular example are those that have, or will have, children that would typically be vaccinated. While the target group may experience long-term consequences of not having their children vaccinated, the children themselves may also suffer significant and sometimes fatal consequences. Likewise, other adults and children may also experience negative consequences, especially if they have not been vaccinated or are immunocompromised.

Something similar may happen in cyber security due to the deployment of a fear appeal. For example, if fear appeals were used to convey the threat of fake anti-malware software and it resulted in individuals being afraid to use legitimate anti-malware software, they could end up having their computer infected, perhaps losing all of their important files or personal photos. Likewise, other computers and systems will also be at risk, even if their owners were not targeted by this fear appeal because infected computers place us all at risk [5]. The point is that it is difficult fully to gauge the long-term consequences of fear appeals, whether in cyber security or elsewhere. What *is* known is that there are numerous unintended consequences of fear appeals, both short and long term [27].

5.3 Other Approaches

Other approaches that engender behavioral change should continue to be explored. This may include providing information on a recommended action without inducing fear. Given the lack of clarity related to which components of a fear appeal (i.e., the fear trigger or the recommended action) are the most effective in causing a change in behavior [36, 37] and the limited number of instances (e.g., [79, 109]) in which cyber security fear appeal studies have examined recommended actions (apart from the fear component), efforts should continue. This is especially true in light of evidence that suggests that the recommended action, by itself, has been both highly effective and more effective overall than presenting threatening information to an individual [152]. Other alternatives to fear appeals, such as those facilitated by *Intervention Mapping* [87], do show some promise.

Another alternative, herd immunity, describes how the immunity of a population or subset of that population works to prevent a larger outbreak from occurring, which results in the larger population being protected [47]. Some consideration should be given to herd immunity in the cyber security context. It may mean that not everyone needs to be compliant or engage in safe cyber security and privacy behaviors [161]. However, this may also result in the *free rider* problem that is seen in the public health sphere—some individuals choosing not to be inoculated since their overall risk has been reduced due to the immunity of the herd [40]. Thus, efforts should continue in parallel between fear appeal approaches and alternatives that use other mechanisms besides fear.

5.4 Conclusion

We provide the guidelines in Section 4.1 to assist researchers trialling fear appeals. Our hope is that subsequent studies will help us to make a more clear-cut judgement about the utility of fear appeals in the cyber security domain.

ACKNOWLEDGMENTS

The authors would like to thank the two shepherds that provided valuable feedback and assistance in the development of the final version of this paper, Aaron Ceross and Simon Parkin. We would also like to thank the anonymous reviewers and NSPW attendees for their invaluable feedback.

REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):41–46, 1999.
[2] D. Albarracín, J. C. Gillette, A. N. Earl, L. R. Glasman, M. R. Durantini, and M.-H. Ho. A test of major assumptions about behavior change: a comprehensive look at the effects of passive and active HIV-prevention interventions since the beginning of the epidemic. *Psychological Bulletin*, 131(6):856–897, 2005.
[3] Y. Albayram, M. M. H. Khan, T. Jensen, and N. Nguyen. "... better to use a lock screen than to worry about saving a few seconds of time": Effect of fear appeal in the context of smartphone locking behavior. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 49–63, 2017.
[4] C. Alwall Svennefelt, E. Hunter, and P. Lundqvist. Evaluating the Swedish approach to motivating improved work safety conditions on farms: insights from fear appeals and the extended parallel processing model. *Journal of Agromedicine*, 23(4):355–373, 2018.
[5] C. L. Anderson and R. Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613–643, 2010.
[6] D. Ariely and M. I. Norton. How actions create–not just reveal–preferences. *Trends in Cognitive Sciences*, 12(1):13–16, 2008.
[7] S. Azagba and M. F. Sharaf. The effect of graphic cigarette warning labels on smoking behavior: evidence from the Canadian experience. *Nicotine & Tobacco Research*, 15(3):708–717, 2012.
[8] A. Bandura. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2):191–215, 1977.
[9] A. Bandura. Perceived self-efficacy in the exercise of control over AIDS infection. *Evaluation and Program Planning*, 13(1):9–17, 1990.
[10] A. Bandura. Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, 52(1):1–26, 2001.
[11] B. Bartikowski, M. Laroche, and M.-O. Richard. A content analysis of fear appeal advertising in Canada, China, and France. *Journal of Business Research*, 103:232–239, October 2019.
[12] K. H. Beck. The effects of risk probability, outcome severity, efficacy of protection and access to protection on decision making: A further test of protection motivation theory. *Social Behavior and Personality: an International Journal*, 12(2):121–125, 1984.
[13] L. S. Beitelspacher, J. D. Hansen, A. C. Johnston, and G. D. Deitz. Exploring Consumer Privacy Concerns and RFID Technology: The Impact of Fear Appeals on Consumer Behaviors. *Journal of Marketing Theory and Practice*, 20(2):147–160, Apr 2012.
[14] B. Berelson and G. A. Steiner. *Human behavior: An inventory of scientific findings*. Harcourt, Brace & World, Oxford, England, 1964.
[15] S. J. Blumberg. Guarding against threatening HIV prevention messages: An information-processing model. *Health Education & Behavior*, 27(6):780–795, 2000.
[16] C. Boshoff and L. Toerien. Subconscious responses to fear-appeal health warnings: An exploratory study of cigarette packaging. *South African Journal of Economic and Management Sciences*, 20(1):1–13, 2017.
[17] S. R. Boss, D. F. 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*, 39(4):837–64, 2015.
[18] F. J. Boster and P. Mongeau. Fear-arousing persuasive messages. *Annals of the International Communication Association*, 8(1):330–375, 1984.
[19] L. Brennan and W. Binney. Fear, guilt, and shame appeals in social marketing. *Journal of Business Research*, 63(2):140–146, 2010.
[20] T. G. Brown, J. Bhatti, and I. Di Leo. Interventions for addiction. In P. M. Miller, editor, *Driving While Impaired (Treatments)*, volume 3, chapter 22. Elsevier Inc., 2013.
[21] D. R. Buchanan. *An ethic for health promotion: rethinking the sources of human well-being*. Oxford University Press, USA, 2000.
[22] D. T. Campbell and J. C. Stanley. *Experimental and quasi-experimental designs for research*. Ravenio Books, Chicago, 2015.
[23] L. Chen and X. Yang. Using EPPM to Evaluate the Effectiveness of Fear Appeal Messages Across Different Media Outlets to Increase the Intention of Breast Self-Examination Among Chinese Women. *Health Communication*, pages 1–8, 2018. https://doi.org/10.1080/10410236.2018.1493416.
[24] M.-F. Chen. Impact of fear appeals on pro-environmental behavior and crucial determinants. *International Journal of Advertising*, 35(1):74–92, 2016.
[25] H. Cho. *Unintended effects of fear appeals: The role of stage of change, threat, and efficacy*. PhD thesis, Mass Media PhD Program, Michigan State University, 1999.
[26] H. Cho and C. T. Salmon. Fear appeals for individuals in different stages of change: Intended and unintended effects and implications on public health campaigns. *Health Communication*, 20(1):91–99, 2006.
[27] H. Cho and C. T. Salmon. Unintended effects of health communication campaigns. *Journal of communication*, 57(2):293–317, 2006.
[28] J. Cohen. *Statistical power analysis for the behavioral sciences*. Routledge Academic, USA, 1988.
[29] S. Cohen and S. D. Pressman. Positive affect and health. *Current Directions in Psychological Science*, 15(3):122–125, 2006.
[30] R. E. Crossler. Protection motivation theory: Understanding determinants to backing up personal data. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, page 10. IEEE, Jan 2010.
[31] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. Future directions for behavioral information security research. *Computers & Security*, 32:90–101, 2013.
[32] J. M. Dabbs Jr and H. Leventhal. Effects of varying the recommendations in a fear-arousing communication. *Journal of Personality and Social Psychology*, 4(5):525–531, 1966.
[33] E. H. Das, J. B. De Wit, and W. Stroebe. Fear appeals motivate acceptance of action recommendations: Evidence for a positive bias in the processing of persuasive messages. *Personality and Social Psychology Bulletin*, 29(5):650–664, 2003.
[34] B. Davis and C. Jansen. This may come as a surprise: How prior knowledge of information in a fear appeal is associated with message outcomes. *Communicatio. South African Journal for Communication Theory and Research*, 42(3):398–421, 2016.
[35] M. de Bruin and G.-J. Y. Peters. Let's not further obscure the debate about fear appeal messages for smokers. *American Journal of Preventive Medicine*, 44(5):e51, 2013.
[36] N. De Hoog, W. Stroebe, and J. B. F. De Wit. The impact of fear appeals on processing and acceptance of action recommendations. *Personality and Social Psychology Bulletin*, 31(1):24–33, 2005.
[37] N. De Hoog, W. Stroebe, and J. B. F. De Wit. The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. *Review of General Psychology*, 11(3):258–285, 2007.
[38] J. P. Dillard. Rethinking the study of fear appeals: An emotional perspective. *Communication Theory*, 4(4):295–323, 1994.
[39] J. P. Dillard, R. Li, E. Meczkowski, C. Yang, and L. Shen. Fear responses to threat appeals: Functional form, methodological considerations, and correspondence between static and dynamic data. *Communication Research*, 44(7):997–1018, 2017.
[40] W. Dimas. Failed Herd Immunity: American Business Compliance and the United States Cyber-Security Policy's Clash with the European Union's General Data Protection Act. *Loyola University Chicago International Law Review*, 15:191–207, 2017.
[41] D. Dolinski and R. Nawrat. "Fear-then-relief" procedure for producing compliance: Beware when the danger is over. *Journal of Experimental Social Psychology*, 34(1):27–50, 1998.
[42] C. Duhigg. *The power of habit: Why we do what we do in life and business*. Random House, London, 2012.
[43] M. Dupuis and R. E. Crossler. The Compromise of One's Personal Information: Trait Affect as an Antecedent in Explaining the Behavior of Individuals. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. IEEE, 2019.
[44] M. Dupuis and S. Khadeer. Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. In *Proceedings of the 5th Annual Conference on Research in Information Technology*, pages 35–40. ACM Press, 2016.
[45] A. Earl and D. Albarracín. Nature, decay, and spiraling of the effects of fear-inducing arguments and HIV counseling and testing: A meta-analysis of the short-and long-term outcomes of HIV-prevention interventions. *Health Psychology*, 26(4):496–506, 2007.
[46] S. Emery, G. Szczypka, E. Abril, Y. Kim, and L. Vera. Are you scared yet? Evaluating fear appeal messages in tweets about the tips campaign. *Journal of Communication*, 64(2):278–295, 2014.

Topic	Pre-FA	Fear Appeal	Post-Fear Appeal				Post-RA Fear	Post-Delay	S'vey Lab Field	Adopt	ExpType
			Perceived (1)	RAF	DC	FC					
Anti-Malware SW [17]	—	EFA, RA	F, Sev, Susc, RE, SE, RC	-	B-OO, BI	MR	-	-	Field	IA	C, R
Compliance [83]	—	EFA, RA	Sev, Susc, RE, SE	-	BI	-	-	-	S'vey	-	Online, C, R
Compliance [66]	—	IFA	Sev, Susc, RE, SE, RC	-	A, BI	-	-	-	S'vey	-	Online
Compliance [82]	—	EFA, RA	Sev, Susc, RE, SE	-	A, BI	-	-	-	S'vey	-	Online, C, R
Data Backups [17]	—	EFA, RA	F, Sev, Susc, RE, SE, RC	-	B-OO, B-SR, BI	-	-	1 term	Field	IA, LTA	R
Data Backups [30]	—	IFA	Sev, Susc, RE, SE, RC	-	B-SR	-	-	-	S'vey	-	Online, In-Person
Org Commitment [138]	—	IFA	F, Sev, Susc, RE, SE, RC	-	B-SR, BI	MR	-	-	S'vey	-	Online
Org Security [175]	SAF	EFA, RA	Sev, Susc, RE, SE	-	BI	-	-	-	Lab	-	fMRI
Personal Information [43]	TAF	IFA	Sev, Susc, RE, SE, RC	-	B-SR	-	-	-	S'vey	-	Online
Phishing [79]	B-SR	EFA, RAP	F, Sev, Susc, RE, SE, RC	-	A, BI, B-SR	MR	(2)	4 wks	S'vey	LTA	Online, C, R
Phone Lock Screen [3]	A, B-SR	EFA, RAP	RE, RC, Sev	-	B-SR	-	-	1 wk	S'vey	LTA	Online, C, R
RFID [13]	—	EFA, RA	Sev, Susc	-	A, BI	-	-	-	S'vey	-	Online, C, R
Ransomware [109]	—	EFA, RA, RAP	Sev, Susc, RE, SE, RC	-	-	MR	-	-	S'vey	-	Online, C, R
PW Compliance [122]	—	EFA, RA, RAP	F, Sev, Susc, RE, SE, RC	-	B-OO, BI	-	-	6 wks	S'vey	IA	Online, C, R
PW Compliance [121]	—	EFA, RAP	Sev, Susc, RE, SE, RC	-	BI	-	-	-	S'vey	-	Online, C, R
PW Reuse [81]	—	EFA, RA	Sev, Susc, RE, SE	-	B-OO, B-SR	-	-	-	Field	IA	Online, C, R
PW Selection [169]	—	EFA, RA, RAP	Sev, Susc, RE, SE, RC	-	B	-	-	-	Field	IA	Online, C, R
Security Adoption [155]	—	EFA, RA	-	-	BI	-	-	-	S'vey	-	Classroom

(1) Only PMT constructs included. (2) PMT constructs used both immediately after the fear appeal and after the delay.

Table 4: Cyber Security Fear Appeal Studies (Acronyms listed in Table 5)

	Meaning		Meaning			Meaning
F/FA	Fear/Fear Appeal	DC	Danger Control	Behavior	B-OO	Objective Observation
RE	Response Efficacy	A	Attitude		B-SR	Self-Report
SE	Self Efficacy	BI	Behavioral Intention	Affect	SAF	State Affect Factor(s)
RC	Response Cost	B	Behavior		TAF	Trait Affect Factor(s)
Sev	Severity	FC	Fear Control	Adopt	IA	Immediate Attempt
Susc	Susceptibility	MR	Maladaptive Rewards		LTA	Long-Term Adoption
EFA	Explicit Fear Appeal	RA	Recommended Action	ExpType	C	Control Included
IFA	Implicit Fear Appeal	RAF	Recommended Action Feasibility		R	Randomized Participants
NFA	No Fear Appeal Used	RAP	Recommended Action Procedures	PW: Password		SW:Software

Table 5: Acronyms used in Table 4

[47] J. M. Epstein. Modelling to contain pandemics. *Nature*, 460(7256):687–688, 2009.

[48] M. Feinberg and R. Willer. The moral roots of environmental attitudes. *Psychological Science*, 24(1):56–62, 2013.

[49] J. Finkenauer and P. W. Gavin. *Scared straight: The panacea phenomenon revisited*. Waveland Press, Prospect Heights, IL, 1999.

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

[51] B. J. Fogg and J. Hreha. Behavior wizard: a method for matching target behaviors with solutions. In *International Conference on Persuasive Technology*, pages 117–131. Springer, 2010.

[52] I. M. Franks and D. Maslovat. The importance of feedback to performance. In *Essentials of Performance Analysis in Sport*, pages 11–17. Routledge, 2015.

[53] D. P. French, E. Cameron, J. S. Benton, C. Deaton, and M. Harvie. Can communicating personalised disease risk promote healthy behaviour change? A systematic review of systematic reviews. *Annals of Behavioral Medicine*, 51(5):718–729, 2017.

[54] N. H. Frijda, P. Kuipers, and E. Ter Schure. Relations among emotion, appraisal, and emotional action readiness. *Journal of Personality and Social Psychology*, 57(2):212–228, 1989.

[55] J. M. George and E. Dane. Affect, emotion, and decision making. *Organizational Behavior and Human Decision Processes*, 136:47–55, 2016.

[56] M. A. Gerend and J. K. Maner. Fear, anger, fruits, and veggies: Interactive effects of emotion and message framing on health behavior. *Health Psychology*, 30(4):420–423, 2011.

[57] S. D. Gottlieb. Vaccine resistances reconsidered: Vaccine skeptics and the Jenny McCarthy effect. *Biosocieties*, 11(2):152–174, 2016.

[58] D. P. Haefner. Arousing fear in dental health education. *Journal of Public Health Dentistry*, 25:140–146, 1965.

[59] C. Haigh and N. A. Jones. An overview of the ethics of cyber-space research and the implication for nurse educators. *Nurse Education Today*, 25(1):3–8, 2005.

[60] T. Halkjelsvik and J. Rise. Disgust in fear appeal anti-smoking advertisements: The effects on attitudes and abstinence motivation. *Drugs: Education, Prevention and Policy*, 22(4):362–369, 2015.

[61] G. Hamilton, D. Cross, and K. Resnicow. Occasional cigarette smokers: Cue for harm reduction smoking education. *Addiction Research*, 8(5):419–437, 2000.

[62] P. Hartmann, V. Apaolaza, C. D'Souza, J. M. Barrutia, and C. Echebarria. Environmental threat appeals in green advertising: The role of fear arousal and coping efficacy. *International Journal of Advertising*, 33(4):741–765, 2014.

[63] G. Hastings, M. Stead, and J. Webb. Fear appeals in social marketing: Strategic and ethical reasons for concern. *Psychology & Marketing*, 21(11):961–986, 2004.

[64] G. Hastings, M. Stead, and J. Webb. Fear appeals in social marketing: Strategic and ethical reasons for concern. *Psychology & Marketing*, 21(11):961–986, 2004.

[65] H. Henson and E. Chang. Locus of control and the fundamental dimensions of moods. *Psychological Reports*, 82(3):1335–8, 1998.

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

[67] M. A. Hewgill and G. R. Miller. Source credibility and response to fear-arousing communications. *Speech Monographs*, 32(2):95–101, 1965.

[68] D. Hill, S. Chapman, and R. Donovan. The return of scare tactics. *Tobacco Control*, 7(1):5–8, 1998.

[69] H. Hoeken, P. Swanepoel, E. Saal, and C. Jansen. Using message form to stimulate conversations: The case of tropes. *Communication Theory*, 19(1):49–65, 2009.

[70] C. D. Hopkins, K. Shanahan, K. M. Hood, and A. White. An Argument for the Use of High Fear Appeals as an Effective Type II Diabetes Health Messaging Strategy: A Structured Abstract. In *Creating Marketing Magic and Innovative Future Marketing Trends*, pages 1193–1197. Springer, 2017.

[71] I. A. Horowitz. Effects of volunteering, fear arousal, and number of communications on attitude change. *Journal of Personality and Social Psychology*, 11(1):34–37, 1969.

[72] I. A. Horowitz. Attitude change as a function of perceived arousal. *The Journal of Social Psychology*, 87(1):117–126, 1972.

[73] I. A. Horowitz and W. E. Gumenik. Effects of the volunteer subject, choice, and fear arousal on attitude change. *Journal of Experimental Social Psychology*, 6(3):293–303, 1970.

[74] C. Hovland, I. Janis, and H. Kelly. *Communication and Persuasion*. Yale University Press, New Haven, 1953.

[75] C. Hunecke, A. Engler, R. Jara-Rojas, and P. M. Poortvliet. Understanding the role of social capital in adoption decisions: An application to irrigation technology. *Agricultural Systems*, 153:221–231, 2017.

[76] M. R. Hyman and R. Tansey. The ethics of psychoactive ads. *Journal of Business Ethics*, 9(2):105–114, 1990.

[77] C. A. Insko, A. Arkoff, and V. M. Insko. Effects of high and low fear-arousing communications upon opinions toward smoking. *Journal of Experimental Social Psychology*, 1(3):256–266, 1965.

[78] I. L. Janis and S. Feshbach. Effects of fear-arousing communications. *The Journal of Abnormal and Social Psychology*, 48(1):78–92, 1953.

[79] J. Jansen and P. van Schaik. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, 123:40–55, Mar 2019.

[80] W. Janssens and P. De Pelsmacker. Fear Appeal in Traffic Safety Advertising: The moderating role of medium context, trait anxiety, and differences between drivers and non-drivers. *Psychologica Belgica*, 47(3):173–193, 2007.

[81] 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*, 20(2):196–213, 2014.

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

[83] 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*, 39(1):113–134, Mar 2015.

[84] S. S. Kegeles, J. P. Kirscht, D. P. Haefner, and I. M. Rosenstock. Survey of beliefs about cancer detection and taking Papanicolaou tests. *Public Health Reports*, 80(9):815–823, 1965.

[85] L. T. Kessels, R. A. Ruiter, and B. M. Jansma. Increased attention but more efficient disengagement: neuroscientific evidence for defensive processing of threatening health information. *Health Psychology*, 29(4):346–354, 2010.

[86] P. M. Kohn, M. S. Goodstadt, G. M. Cook, M. Sheppard, and G. Chan. Ineffectiveness of threat appeals about drinking and driving. *Accident Analysis & Prevention*, 14(6):457–464, 1982.

[87] G. Kok, N. H. Gottlieb, G.-J. Y. Peters, P. D. Mullen, G. S. Parcel, R. A. Ruiter, M. E. Fernández, C. Markham, and L. K. Bartholomew. A taxonomy of behaviour change methods: an intervention mapping approach. *Health Psychology Review*, 10(3):297–312, 2016.

[88] G. Kok, G.-J. Y. Peters, L. T. Kessels, G. A. Ten Hoor, and R. A. Ruiter. Ignoring theory and misinterpreting evidence: the false belief in fear appeals. *Health Psychology Review*, 12(2):111–125, 2018.

[89] S. Kraus, E. El-Assal, and M. L. de Fleur. Fear-threat appeals in mass communication: An apparent contradiction. *Communications Monographs*, 33(1):23–29, 1966.

[90] H. P. Krisher, S. A. Darley, and J. M. Darley. Fear-provoking recommendations, intentions to take preventive actions, and actual preventive actions. *Journal of Personality and Social Psychology*, 26(2):301–308, 1973.

[91] K. Krol, J. M. Spring, S. Parkin, and M. A. Sasse. Towards robust experimental design for user studies in security and privacy. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*, pages 21–31, 2016.

[92] A. Lang and N. S. Yegiyan. Understanding the interactive effects of emotional appeal and claim strength in health messages. *Journal of Broadcasting & Electronic Media*, 52(3):432–447, 2008.

[93] M. S. LaTour and H. J. Rotfeld. There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Advertising*, 26(3):45–59, 1997.

[94] J. Lau, A. Lee, S. Wai, P. Mo, F. Fong, Z. Wang, L. Cameron, and V. Sheer. A randomized control trial for evaluating efficacies of two online cognitive interventions with and without fear-appeal imagery approaches in preventing unprotected anal sex among Chinese men who have sex with men. *AIDS and Behavior*, 20(9):1851–1862, 2016.

[95] S. T. Lawson, S. K. Yeo, and E. Greene. The cyber-doom effect: The impact of fear appeals in the us cyber security debate. In *Proceedings of the 8th International Conference on Cyber Conflict*, pages 65–80. NATO CCO COE Publications, May 2016.

[96] R. Lennon, R. Rentfro, and B. O'Leary. Social marketing and distracted marketing and distracted driving behaviors among young adults: The effectiveness of fear appeals. *Academy of Marketing Studies Journal*, 14(2):95–113, 2010.

[97] H. Leventhal. Findings and theory in the study of fear communications. In *Advances in Experimental Social Psychology*, volume 5, pages 119–186. Elsevier, 1970.

[98] H. Leventhal, R. Singer, and S. Jones. Effects of fear and specificity of recommendation upon attitudes and behavior. *Journal of Personality and Social Psychology*, 2(1):20–29, 1965.

[99] H. Leventhal and J. C. Watts. Sources of resistance to fear-arousing communications on smoking and lung cancer. *Journal of Personality*, 34(2):155–175, 1966.

[100] H. Leventhal, J. C. Watts, and F. Pagano. Effects of fear and instructions on how to cope with danger. *Journal of Personality and Social Psychology*, 6(3):313–321, 1967.

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

[102] I. Lewis, B. Watson, and K. M. White. An examination of message-relevant affect in road safety messages: Should road safety advertisements aim to make us feel good or bad? *Transportation Research Part F: Traffic Psychology and Behaviour*, 11(6):403–417, 2008.

[103] I. M. Lewis, B. Watson, K. M. White, and R. Tay. Promoting public health messages: Should we move beyond fear-evoking appeals in road safety? *Qualitative Health Research*, 17(1):61–74, 2007.

[104] I. Lynch, L. M. De Bruin, N. Cassimjee, and C. Wagner. A qualitative investigation of South African cigarette smokers' perceptions of fear appeal messages in anti-smoking advertising advertising. *Health SA Gesondheid*, 14(1), 2009.

[105] J. T. MacCurdy. *The Structure of Morale*. Cambridge University Press, New York, 1943.

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

[107] M. A. Mahmood, M. Siponen, D. Straub, H. R. Rao, and T. Raghu. Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly*, 34(3):431–433, 2010.

[108] E. W. Maibach, M. Nisbet, P. Baldwin, K. Akerlof, and G. Diao. Reframing climate change as a public health issue: an exploratory study of public reactions. *BMC Public Health*, 10(1):299–310, 2010.

[109] K. Marett, A. Vedadi, and A. Durcikova. A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses. *Computers & Security*, 80:25–35, Jan 2019.

[110] R. Markšaitytė, D. Šakinytė, L. Šeibokaitė, A. Endriulaitienė, K. Žardeckaitė-Matulaitienė, and J. Slavinskienė. The road safety advertisements targeting drunk driving: Do threat appeals actually arouse fear? In *Proceedings of the 22nd International Scientific Conference. Transport Means. Part 1. Kaunas University of Technology [Vol. 22 (1)]*, Trakai, Lithuania, October 3-5 2018.

[111] M. L. Markus and D. Robey. Information technology and organizational change: causal structure in theory and research. *Management Science*, 34(5):583–598, 1988.

[112] S. Mayor. Baby doll simulation scheme does not reduce teen pregnancies, study finds. *British Medical Journal*, 354, 2016.

[113] A. McCluskey and M. Lovarini. Providing education on evidence-based practice improved knowledge but did not change behaviour: a before and after study. *BMC Medical Education*, 5(1):40, 2005.

[114] W. McGuire. Personality and attitude change: An information processing theory. In A. G. Greenwald, T. C. Brock, and T. M. Ostrom, editors, *Psychological Foundations of Attitudes*, pages 171–196. Academic Press, 1968.

[115] B. A. Mellers. Choice and the relative pleasure of consequences. *Psychological Bulletin*, 126(6):910–924, 2000.

[116] J. S. Mill. Utilitarianism (1863). *Utilitarianism, Liberty, Representative Government*, pages 7–9, 1859.

[117] N. E. Miller. Studies of fear as an acquirable drive: I. Fear as motivation and fear-reduction as reinforcement in the learning of new responses. *Journal of Experimental Psychology*, 38(1):89–101, 1948.

[118] 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*, 30(1):106–143, 2000.

[119] M. Mostafa. Neural correlates of fear appeal in advertising: An fMRI analysis. *Journal of Marketing Communications*, pages 1–25, 2018.

[120] N. Muthusamy, T. R. Levine, and R. Weber. Scaring the already scared: Some problems with HIV/AIDS fear appeals in Namibia. *Journal of Communication*, 59(2):317–344, 2009.

[121] 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*, pages 3188–3197. IEEE, Jan 2014.

[122] 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*, 42(7):147–182, Feb 2018.

[123] R. L. Nabi, D. Roskos-Ewoldsen, and F. Dillman Carpentier. Subjective knowledge and fear appeal effectiveness: Implications for message design. *Health Communication*, 23(2):191–201, 2008.

[124] D. J. O'Keefe. *Persuasion: Theory and research*, volume 2. Sage, Thousand Oaks, 2002.

[125] D. J. O'Keefe. Misunderstandings of effect sizes in message effects research. *Communication Methods and Measures*, 11(3):210–219, 2017.

[126] M. T. O'Keefe. The anti-smoking commercials: A study of television's impact on behavior. *The Public Opinion Quarterly*, 35(2):242–248, 1971.

[127] S. O'Neill and S. Nicholson-Cole. "Fear won't do it" promoting positive engagement with climate change through visual and iconic representations. *Science Communication*, 30(3):355–379, 2009.

[128] J. R. Ordoñana, F. Gonzalez-Javier, L. Espín-López, and J. Gómez-Amor. Self-report and psychophysiological responses to fear appeals. *Human Communication Research*, 35(2):195–220, 2009.

[129] A. Ort and A. Fahr. Using efficacy cues in persuasive health communication is more effective than employing threats–An experimental study of a vaccination intervention against Ebola. *British Journal of Health Psychology*, 23(3):665–684, 2018.

[130] A. Ortony and T. J. Turner. What's basic about basic emotions? *Psychological Review*, 97(3):315–331, 1990.

[131] J. W. Out and K. D. Lafreniere. Baby Think It Over (R): Using role-play to prevent teen pregnancy. *Adolescence*, 36(143):571–82, 2001.

[132] G.-J. Y. Peters, M. De Bruin, and R. Crutzen. Everything should be as simple as possible, but no simpler: towards a protocol for accumulating evidence regarding the active content of health behaviour change interventions. *Health Psychology Review*, 9(1):1–14, 2015.

[133] G.-J. Y. Peters, R. A. Ruiter, and G. Kok. Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review*, 7(sup1):S8–S31, 2013.

[134] G.-J. Y. Peters, R. A. Ruiter, and G. Kok. Threatening communication: A qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals. *International Journal of Psychology*, 49(2):71–79, 2014.

[135] A. Petrosino, C. Turpin-Petrosino, and J. O. Finckenauer. Well-meaning programs can have harmful effects! Lessons from experiments of programs such as Scared Straight. *Crime & Delinquency*, 46(3):354–379, 2000.

[136] E. S. Poole, M. Chetty, T. Morgan, R. E. Grinter, and W. K. Edwards. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 739–748. ACM, 2009.

[137] L. Popova. The extended parallel process model: Illuminating the gaps in research. *Health Education & Behavior*, 39(4):455–473, 2012.

[138] C. Posey, T. L. Roberts, and P. B. Lowry. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4):179–214, 2015.

[139] J. H. Price, J. A. Dake, J. Murnan, J. Dimmig, and S. Akpanudo. Power analysis in survey research: Importance and use for health educators. *American Journal of Health Education*, 36(4):202–207, Aug 2005.

[140] D. W. Putwain, G. Nakhla, A. Liversidge, L. J. Nicholson, B. Porter, and M. Reece. Teachers use of fear appeals prior to a high-stakes examination: Is frequency linked to perceived student engagement and how do students respond? *Teaching and Teacher Education*, 61:73–83, 2017.

[141] D. W. Putwain, W. Symes, and H. M. Wilkinson. Fear appeals, engagement, and examination performance: The role of challenge and threat appraisals. *British Journal of Educational Psychology*, 87(1):16–31, 2017.

[142] S. Radelfinger. Some effects of fear-arousing communications on preventive health behavior. *Health Education Monographs*, 1(19):2–15, 1965.

[143] J. D. Ragsdale and K. R. Durham. Audience response to religious fear appeals. *Review of Religious Research*, 28(1):40–50, 1986.

[144] K. Renaud, R. Otondo, and M. Warkentin. "This is the way 'I' create my passwords"... does the endowment effect deter people from changing the way they create their passwords? *Computers & Security*, 82:241–260, 2019.

[145] N. Rhodes. Fear-appeal messages: Message processing and affective attitudes. *Communication Research*, 44(7):952–975, 2017.

[146] R. N. Rimal. Perceived risk and self-efficacy as motivators: Understanding individuals' long-term use of health information. *Journal of Communication*, 51(4):633–654, 2001.

[147] P. A. Rippetoe and R. W. Rogers. Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3):596–604, 1987.

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

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

[150] R. W. Rogers and C. R. Mewborn. Fear appeals and attitude change: effects of a threat's noxiousness, probability of occurrence, and the efficacy of coping responses. *Journal of Personality and Social Psychology*, 34(1):54–61, 1976.

[151] A. Rosenberg. *Philosophy of science: A contemporary introduction*. Routledge, London and New York, 2011.

[152] R. Ruiter, L. Kessels, G. Peters, and G. Kok. Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, 49(2):63–70, 2014.

[153] R. A. Ruiter, C. Abraham, and G. Kok. Scary warnings and rational precautions: A review of the psychology of fear appeals. *Psychology and Health*, 16(6):613–630, 2001.

[154] L. Shen and E. Bigsby. *The SAGE handbook of persuasion developments in theory and practice*. Sage, Thousand Oaks, Calif, 2012.

[155] J. D. Shropshire, M. Warkentin, and A. C. Johnston. Impact of negative message framing on security adoption. *Journal of Computer Information Systems*, 51(1):41–51, 2010.

[156] N. R. Simonson and R. M. Lundy. The effectiveness of persuasive communication presented under conditions of irrelevant fear. *Journal of Communication*, 16(1):32–37, 1966.

[157] J. K. Simpson. Appeal to fear in health care: appropriate or inappropriate? *Chiropractic & Manual Therapies*, 25(27):1–10, 2017.

[158] S. Slavin, C. Batrouney, and D. Murphy. Fear appeals and treatment side-effects: an effective combination for HIV prevention? *AIDS Care*, 19(1):130–137, 2007.

[159] R. D. Stainback and R. W. Rogers. Identifying effective components of alcohol abuse prevention programs: Effects of fear appeals, message style, and source expertise. *International Journal of the Addictions*, 18(3):393–405, 1983.

[160] B. Sternthal and C. S. Craig. Fear appeals: Revisited and revised. *Journal of Consumer Research*, 1(3):22–34, 1974.

[161] C. E. Stewart, A. M. Vasu, and E. Keller. Communityguard: A crowdsourced home cyber-security system. In *Proceedings of the ACM International workshop on security in software defined networks & network function virtualization*, pages 1–6. ACM, 2017.

[162] D. Straub. Black hat, white hat studies in information security. *Keynote Presentation of the Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.n*, 8, 2009.

[163] S. Sutton and J. Eiser. The effect of fear-arousing communications on cigarette smoking: An expectancy-value approach. *Journal of Behavioral Medicine*, 7(1):13–33, 1984.
[164] K. Sweeny, D. Melnyk, W. Miller, and J. A. Shepperd. Information avoidance: Who, what, when, and why. *Review of General Psychology*, 14(4):340–353, 2010.
[165] M. B. Tannenbaum, J. Hepler, R. S. Zimmerman, L. Saul, S. Jacobs, K. Wilson, and D. Albarracín. Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, 141(6):1178–1204, 2015.
[166] P.-A. Tengland. Behavior change or empowerment: on the ethics of health-promotion strategies. *Public Health Ethics*, 5(2):140–153, 2012.
[167] M. Terblanche-Smit and N. Terblanche. The effect of fear appeal HIV/AIDS social Marketing on Behavior: Evaluating the Importance of Market Segmentation. In *9th International Congress of the International Association on Public and Non-Profit*, pages 31–38, 2010.
[168] J. F. Tunner Jr, E. Day, and M. R. Crask. Protection motivation theory: An extension of fear appeals theory in communication. *Journal of Business Research*, 19(4):267–276, 1989.
[169] A. Vance, D. Eargle, K. Ouimet, and D. Straub. Enhancing password security through interactive fear appeals: A web-based field experiment. In *46th Hawaii International Conference on System Sciences (HICSS)*, pages 2988–2997, 2013.
[170] K. E. Vaniea, E. Rader, and R. Wash. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2671–2674. ACM, 2014.
[171] J. van't Riet and R. A. Ruiter. Defensive reactions to health-promoting information: An overview and implications for future research. *Health Psychology Review*, 7(sup1):S104–S136, 2013.
[172] D. Västfjäll, P. Slovic, W. J. Burns, A. Erlandsson, L. Koppel, E. Asutay, and G. Tinghög. The arithmetic of emotion: Integration of incidental and integral affect in judgments and decisions. *Frontiers in Psychology*, 7:325, 2016. doi: 10.3389/fpsyg.2016.00325.
[173] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3):576–586, 2011.
[174] M. Warkentin, D. Straub, and K. Malimage. Featured talk: Measuring secure behavior: A research commentary. In *Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY*, 2012.
[175] M. Warkentin, E. Walden, A. Johnston, and D. Straub. Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems*, 17(3):194–215, Mar 2016.
[176] D. Watson and L. A. Clark. The PANAS-X: Manual for the Positive and Negative Affect Schedule - Expanded Form, 1994. University of Iowa.
[177] N. D. Weinstein. Perceived probability, perceived severity, and health-protective behavior. *Health Psychology*, 19(1):65–74, 2000.
[178] K. Witte. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4):329–349, 1992.
[179] K. Witte. Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In *Handbook of Communication and Emotion*, pages 423–450. Elsevier, 1996.
[180] K. Witte and M. Allen. A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, 27(5):591–615, 2000.
[181] K. Witte, G. Meyer, and D. Martell. *Effective health risk messages: A step-by-step guide.* Sage, Thousand Oaks, 2001.
[182] Ł. P. Wojciechowski and V. Babjaková. Necromarketing in the Media and Marketing Communications. *Social Communication*, 2(2):15–29, Oct 2015.
[183] M. C. Yzer, B. G. Southwell, and M. T. Stephenson. Inducing fear as a public communication campaign strategy. In R. E. Rice and C. K. Atkin, editors, *Public Communication Campaigns*, pages 163–176. Sage, Thousand Oaks, CA, 4 edition, 2012.