Ethics and Information Technology
https://doi.org/10.1007/s10676-020-09560-0

ORIGINAL PAPER

Scoping the ethical principles of cybersecurity fear appeals

Marc Dupuis[1] · **Karen Renaud**[2]

Abstract
Fear appeals are used in many domains. Cybersecurity researchers are also starting to experiment with fear appeals, many reporting positive outcomes. Yet there are ethical concerns related to the use of fear to motivate action. In this paper, we explore this aspect from the perspectives of cybersecurity fear appeal *deployers* and *recipients*. We commenced our investigation by considering fear appeals from three foundational ethical perspectives. We then consulted the two stakeholder groups to gain insights into the ethical concerns they consider to be pertinent. We first consulted *deployers*: (a) fear appeal researchers and (b) Chief Information Security Officers (CISOs), and then potential cybersecurity fear appeal *recipients:* members of a crowdsourcing platform. We used their responses to develop an *effects-reasoning matrix*, identifying the potential benefits and detriments of cybersecurity fear appeals for all stakeholders. Using these insights, we derived six ethical principles to guide cybersecurity fear appeal deployment. We then evaluated a snapshot of cybersecurity studies using the ethical principle lens. Our contribution is, *first*, a list of potential detriments that could result from the deployment of cybersecurity fear appeals and *second*, the set of six ethical principles to inform the deployment of such appeals. Both of these are intended to inform cybersecurity fear appeal design and deployment.

Keywords Fear appeals · Cybersecurity · Ethics · Ethical principles

Introduction

Fear is defined by Walton (2010, p. 178), as *an emotion that moves people powerfully to action, and may tend to make them put more careful considerations of the complex features of a situation aside*. A fear appeal usually packages some fear "trigger", together with an action that the fear appeal designer wants the recipient to take. The consequence, so the theory goes, is that the fear appeal recipient will seek to reduce the negative emotion by taking the recommended action (Frijda et al. 1989).

Fear appeals have spread from use in religion (Ragsdale and Durham 1986) (centuries) to a variety of other domains, including smoking (Hamilton et al. 2000), nuclear radiation (Dillard 1994), alcohol abuse (Stainback and Rogers 1983) and, recently, cybersecurity[1] (Johnston and Warkentin 2010; Johnston et al. 2015; Vance et al. 2013).

Fear appeals are delivered via a variety of channels including, for example, on cigarette packets, in health practitioners' waiting rooms and via a computer's user interface (Fig. 1[2]).

While many advocate the use of fear appeals (Johnston and Warkentin 2010; Johnston et al. 2015; Vance et al. 2013; Beck 1984; Stainback and Rogers 1983; Tannenbaum et al. 2015), others argue that fear appeals are actually ill-advised, harmful, or ineffective (Albarracín et al. 2005; Brennan and Binney 2010; Kok et al. 2018; Kohn et al. 1982; Krisher et al. 1973; Lau et al. 2016; Hastings et al. 2004) and others warn against the use of fear in behavioral interventions (Brennan and Binney 2010; Lewis et al. 2008; O'Neill and Nicholson-Cole 2009), with a number citing ethical concerns (Tengland 2012; Hastings et al. 2004; Hyman and Tansey 1990). Given the differences of opinion, it seems

✉ Marc Dupuis
marcjd@uw.edu

Karen Renaud
k.renaud@abertay.ac.uk

1 Computing and Software Systems, University of Washington, Box 358534, Bothell, WA 98011, USA

2 School of Design and Informatics, Abertay University, Bell Street, Dundee, Scotland DD1 1HG, UK

[1] http://www.accountingdegree.com/blog/2012/mobile-commerce-crime-10-scary-trends-to-watch-out-for/; https://www.gflesch.com/blog/scary-cybersecurity-facts.

[2] Ur et al. (2017), https://www.publichealth.hscni.net/publications/measles-dont-let-your-child-catch-it-poster.

Published online: 20 October 2020

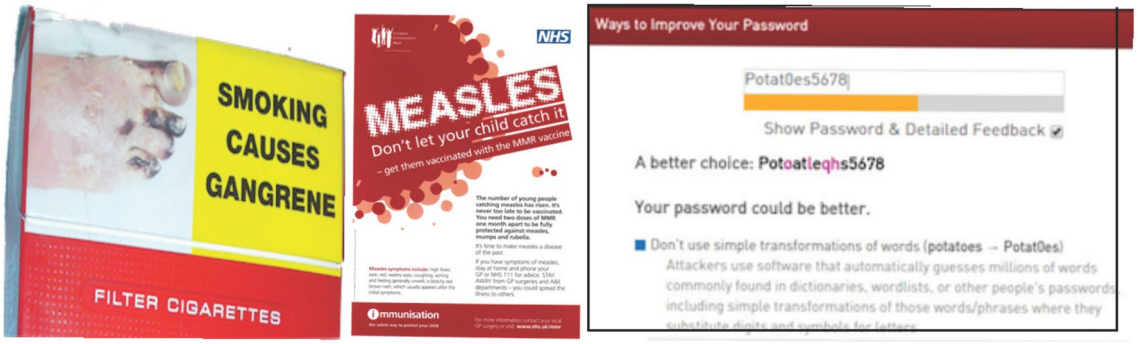


Fig. 1 Fear appeal examples (cigarettes, contagious disease and poor password choice)

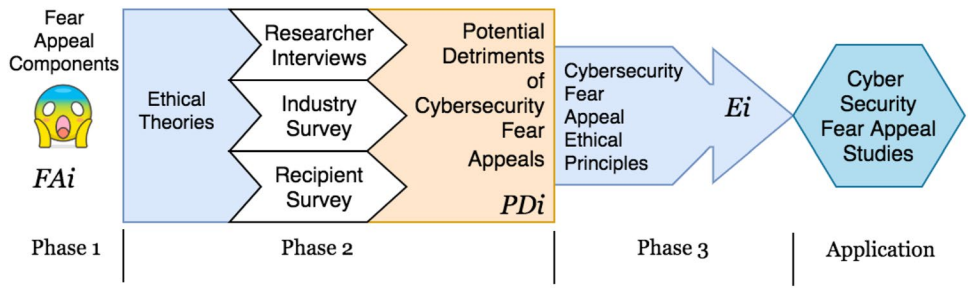


Fig. 2 The phases involved in this research

appropriate to contemplate the ethical implications of cybersecurity fear appeals. As depicted in Fig. 2, the paper is structured as follows:

In *Phase 1*, we commence by explaining what a fear appeal is, detail its constituent parts (*FAi*) and introduce three different ethical theories, which provide a useful lens in considering the ethics of fear appeals (section "Phase 1: Theory").

In *Phase 2*, we detail the methods and materials used in our study (section "Phase 2: Material and methods"). Next, we report on the insights gained from interviews we carried out with fear appeal researchers, a survey with company Chief Information Security Officers (CISOs) and members of the public, in order to identify their perceptions of the potential detriments of fear appeal deployment—*PDi* (section "Phase 2: Results"). We chose to interview these particular stakeholders because researchers carry out research to test the efficacy and design features of fear appeals. Their findings are likely to feed into the use of cybersecurity fear appeals by CISOs within their organizations to encourage secure behaviors. We also surveyed members of the public, as the main targets of such cybersecurity fear appeals, to ensure that we gauged perceptions from both deployers and their target audience.

The selection of these stakeholders was designed to be complementary to one another since the questions we asked and the perspectives they represented are all quite different from one another. Thus, the goal was breadth of perspective rather than depth with a singular focus. We do not suggest that the perspectives and insight gleaned from these stakeholders is generalizable to other types of stakeholders or similar stakeholders of the same type. Instead, our focus was to better understand some of the concerns and opinions related to the use of fear appeals from a diverse group of stakeholder types in a complementary manner.

We analyzed the outcomes of the interviews and surveys to extract benefits and potential detriments (*PDi*) of cybersecurity fear appeal deployment. We developed an Effects-Reasoning Matrix (ERM), a mechanism proposed by Duke et al. (1993), to evaluate and depict the benefits and potential detriments of cybersecurity fear appeals (Duke et al. 1993). Duke *et al.*explain that this matrix *is intended to aid in isolating and identifying conflicts that may arise when fear appeals are considered from a variety of ethical perspectives involving many interested publics* [p. 120].

In *Phase 3*, we build on the insights we gained during phase 2 to derive six ethical principles to inform the deployment of cybersecurity fear appeals—*Ei* (section "Phase 3: Deriving ethical principles (*Ei*)"). These build on the fear appeal components (*FAi*) enumerated in section "Fear appeals (FAi)", the ethical insights from section "Ethical theories", and the potential detriments that emerged from phase 2 (*PDi*).

Application: We subsequently used the ethical principle lens to review a representative sample of cybersecurity fear appeal studies.

Finally: We consolidate our insights to reflect on the ethics of cybersecurity fear appeals and the limitations of this study in section "Reflection" and conclude in section "Conclusion".

Phase 1: Theory

Fear appeals (FAi)

The essential components of fear appeals (*FAi*) are as follows, ordered as recommended by Dillard et al. (2017), Leventhal (1970).

FA1 Information about the importance of a **threat** (*triggering fear* (Leventhal 1970)) and the *cause*. Also details about the *consequence* of the threat, emphasizing the *severity* thereof (Tannenbaum et al. 2015; Rogers and Mewborn 1976; De Hoog et al. 2007) e.g. "you could lose all your personal photos."

FA2 Explaining that the recommended action has **response efficacy** (*action will be effective in mitigating the threat* (Dillard et al. 2017; Lewis et al. 2008; Tunner et al. 1989)) e.g." making regular backups ensure that your photos will always be there for you."

FA3 Exact details related to feasible **recommended actions** to be taken to reduce or remove the threat (*how to assuage the fear* (Leventhal 1970; Witte 1992; Lawson et al. 2016)) e.g. "register for a cloud backup service and set up auto-backup on your devices, as follows..."

FA4 A statement related to their ability to take the action: **self-efficacy** (*the individual's belief in being able to take the action* (Dillard et al. 2017; Dabbs and Leventhal 1966; Hamilton et al. 2000; Emery et al. 2014; Bandura 2001; Hartmann et al. 2014; Peters et al. 2013; Bandura 1977)) e.g. "98% of people using this backup service rate it as extremely easy to use." Dillard *et al.*explain that people will take desirable actions if they *are able to do so* (Dillard 1994), making perceived self efficacy essential.

Fear appeal theories

Theories that explain how fear engenders behavioral change include: (1) *Fear as Drive* (Hovland et al. 1953), (2) *Parallel Response Model* (Leventhal 1970), considering that fear triggers two independent processes: fear control and danger control. The next two theories elaborate this initial model: *Protection Motivation Theory (PMT)* (Rogers 1975), and (4) *Extended Parallel Process Model* (Witte 1992). These all incorporate some notion of fear being triggered, leading to an appraisal of the threat and the efficacy of the recommended action as a response. The recipient also considers their own competence in terms of carrying out the recommended action. These theories explain how fear appeals influence behavior but are not intended to address the ethical considerations of their deployment. As such, they cannot answer our primary research questions.

Fear appeal efficacy

Cybersecurity fear appeals have been used with varying measures of success, either to persuade people to cease or reduce ill-advised behaviors, or to commence secure behaviors (Beck 1984; Stainback and Rogers 1983; Tannenbaum et al. 2015).

Yet there are those who consider fear appeals ill-advised (Arthur and Quester 2003; Brennan and Binney 2010; Kok et al. 2018; Kohn et al. 1982; Krisher et al. 1973; Lau et al. 2016). Kok et al. (2018) deplores the general "false belief" in fear appeals. French et al. (2017) find little evidence that risk information impacts health behaviors. Peters et al. (2014) call fear "a bad counselor". These concerns come from researchers and practitioners working in other domains but need also to be considered in the cybersecurity domain (Renaud and Dupuis 2019).

Whenever this kind of dissent manifests around the use of a particular behavioral intervention, we can turn to ethical theories to help us to decide whether to proceed with its deployment, or not.

Ethical theories

Cavanagh et al. (1981) argue for consideration of three kinds of moral theories in contemplating the ethics of a proposed action: (1) *theory of rights*, (2) *utilitarian* and (3) *theories of justice*.

(1) The *theory of rights* is argued by Kant, whose three principles of morality are encapsulated in his "categorical imperative" (Reynolds and Bowie 2004; Duke et al. 1993):

   i. *The Golden Rule* only do to others what you would like others to do to you.
   ii. *Respect for Humanity* humans should not be used as means to an end; humans have basic human rights and are an end in themselves;
   iii. *Universality* the action should be universally acceptable to all human beings.

(2) *Utilitarian* theories (Mill and Utilitarianism 1863) argue that the benefits obtained from an action, such as a positive change in behavior, outweigh the costs.

(3) *Theories of justice* are linked to public reasoning, the idea that there are rules which reasonable agents would agree to be subject to Rawls (2005). Wrapped up in Rawls' conceptualization of justice is that everyone in society ought to consider that they are being treated fairly by an intervention.

We can now consider fear appeals under the umbrella of each of these three ethical theories:

Cybersecurity fear appeals under Kant

Kant's categorical imperative is: *Act only according to that rule whereby you can, at the same time, will that it should become a universal law.* (Thompson 2012, p. 629). This approach mandates respect for the autonomy of decision makers. There is also an absolute requirement for recipients to be given requisite knowledge about the risks and to be allowed to consent to receive the risk communication.

The goal of fear appeals is to derive positive behavioral outcomes. Those results naturally frame the use of fear appeals. There is clearly an important role for the users of systems to behave in such a way as to minimize cybersecurity risks. However, Kantian ethics is concerned with the act itself (Micewski and Troy 2007) and, as such, is not inherently concerned with, or otherwise focused on, the possible outcome of the act. Basically, the argument is that people should not be manipulated in order to achieve some other end, such as a desired behavior. Indeed, one of Kant's arguments is that people should never be treated as a means to an end, in this case better cybersecurity for society.

There are a number of arguments opposing the use of fear under Kantian ethics. For example, Bayer and Fairchild (2016) consider fear appeals to be inherently paternalistic, disempowering the recipient, and compromising their agency and autonomy. This is similar to the increased role of technology in our lives (Royakkers et al. 2018). Inducing fear in individuals may result in unsafe levels of anxiety and tension for some, especially among those that already have a mental health condition (Hastings et al. 2004; Hyman and Tansey 1990) or are of a particular age (Benet et al. 1993). We could ask whether the mere possibility of encouraging a target behavior serves a greater good than the very probable outcome of one or more individuals experiencing real psychological harm, especially when the fear arousal is particularly high. Considering the greater perceived efficacy of high-level fear appeals compared with low-level fear appeals (Emery et al. 2014; Hartmann et al. 2014), this suggests that the former is more likely to be used. However, it is also these high-level fear appeals that are most likely to cause psychological harm (Berelson and Steiner 1964; Chen 2016; Janis and Feshbach 1953). Those who disapprove of the use of fear appeals may consider that cybersecurity education, training, and awareness programs should be used to improve outcomes but that these should not be used within a fear appeal.

There are also arguments against applying Kantian ethics to cybersecurity fear appeals. It may be argued that the categorical imperative is inherently subjectively applied. As such, it is entirely possible for one person to approve of the use of fear appeals, and their becoming a universal way of motivating action. Another person may consider them abhorrent. We next consider the Utilitarian perspective.

Cybersecurity fear appeals under utilitarianism

Utilitarian ethics provides a contrasting viewpoint on behavior, intent, and outcome (West 2004). The mantra here is: *Do that which produces the greatest good for the greatest number of affected parties.* (Thompson 2012, p. 629). The outcome of an action is what is important in utilitarianism; it is a type of consequentialism ethics (Buchanan and Ess 2008). The central question of whether an action is ethical or not rests on whether it improves happiness or decreases unhappiness, for the populace as a whole.

For a utilitarian, risk communication should focus on achieving desired outcomes. Facilitating a detailed understanding of the risks is not required (Thompson 2012). If a positive outcome is achieved as measured by its effect on the populace as a whole, then how this was achieved is of little concern so long as these benefits outweigh the costs.

Utilitarian ethics is the ethical framework that guides human subjects research in the United States (Capurro and Pingel 2002) and is even codified in law (Buchanan and Ess 2008). According to the U.S. Code of Federal Regulations, *Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result* (32 CFR Ch. I, Section 219.111(a)(2)). The possible benefits to a research participant are not mandatory; instead, the law looks at the big picture. If the benefits do not outweigh the costs associated with its derivation for a participant in a study, then it is acceptable, so long as the knowledge gained does.

Cybersecurity research is often focused on how an organization or the Internet community as a whole may be made safer by conducting research on the individual (e.g., Anderson and Agarwal 2010), rather than merely by how a particular individual can engage in safer online behavior for herself. Both foci are important, but the result may be such that there is little, if any, discernible benefit for a single individual participating in a cybersecurity fear appeal study, at least in the short-term. The greater hope is that any costs incurred by the participant, whether psychological or otherwise, are far outweighed by the potential benefits to a much larger audience. In this respect, cybersecurity fear appeal research generally operates from a utilitarian ethics framework.

Cybersecurity fear appeals under justice theory

The mantra here is that any intervention should be fair, and accepted as such by the population as a whole. For example, the prohibition of alcohol in the USA was initially supported by citizens (Graham 2019) but became increasingly unpopular due to dissatisfaction with the stringent activities the state used to enforce prohibition (Cowan 1986). The act was eventually repealed, even though there is evidence that prohibition did indeed reduce rates of liver cirrhosis and infant mortality (Moore 1989).

In the realms of fear appeals there is also concern from a justice perspective. Furedi (2018) warn that the creation of a culture of fear could be corrosive to society, leading to a general level of mistrust. Arthur and Quester (2003) carried out a study to compare different kinds of fear appeals and found that participants found social threat type fear appeals the most unethical.

One ethical dilemma is the demonization that may occur when specific subgroups are targeted with a fear appeal. This occurred during the height of the AIDS crisis during which fear appeal messages led people to further stigmatize and demonize gay individuals (Wojciechowski and Babjaková 2015). The very group the message is intended to help the most may actually be harmed through this demonization. Furedi (2018) argues that people can start to see risk avoidance, which is what fear appeals try to achieve, as a moral duty. This means that those who refuse to succumb to fear appeals could end up being marginalized by society.

Perhaps equally as troubling, this demonization may lead to complacency among those that are not within the subgroup (Hastings et al. 2004). When the focus is on one particular subgroup, it means other subgroups may feel as if the message does not apply to them. While it may make sense to target the higher-risk subgroups, it may ultimately send the wrong message. For example, campaigns targeting sexually transmitted infections have often focused on subgroups considered more sexually active (e.g., younger individuals) and those likely to engage in unsafe sexual practices, such as not using a condom. This has arguably resulted in increased rates of sexually transmitted infections among older adults (Minichiello et al. 2012). After all, they may feel that if they were at risk then the messaging would target them as well.

Given that fear appeals are often used to elicit a change in behavior from a group of people that are at some risk based on their current behavior, it is not surprising that many targets of fear appeals belong to one or more inherently vulnerable groups. For example, fear appeals may be used to help elderly individuals engage in behavior that is safer for them (Benet et al. 1993). The intent may be worthwhile, but in effect we are trying to scare an already vulnerable group. Even if it works, is it ethical to scare any group of people for this desired end, let alone a group that may already be vulnerable? Indeed, Watney (1989) raises concerns about fear appeals terrorizing those that they are targeting.

In terms of fairness, it is easy to see that issues might well emerge with the use of fear appeals in any heterogeneous and diverse population.

Phase 2: Material and methods

Duke et al. (1993) suggest examining the ethics of fear appeals by considering the benefits and detriments to all stakeholders. We thus consulted two cybersecurity fear appeal stakeholders: (1) *deployers*: fear appeal researchers and organizational CISOs, and (2) *recipients*: the potential targets of such fear appeals. IRB approval was on file and informed consent was obtained in all instances.

Cybersecurity fear appeal deployer opinions

Our primary research questions were:

RQ1 Does the deployer approve of the use of cybersecurity fear appeals to motivate secure behaviors?

RQ2 Does the deployer consider cybersecurity fear appeals to be efficacious in motivating secure behaviors?

RQ3 Which ethical issues are raised about the use of cybersecurity fear appeals to motivate secure behaviors?

Recruitment: deployers

We identified a number of cybersecurity fear appeal researchers based on their authorship of highly-cited cybersecurity fear appeal papers. We emailed these to request a Skype-based interview, explaining what our study was about. We carried out semi-structured interviews, remotely via Skype, with the six researchers who agreed, asking the questions provided in Appendix B. All of these are located within the UK or the USA.

We invited CISOs to take our survey, once again relying on convenience sampling. The survey consisted of both quantitative and qualitative questions. Eleven CISOs representing both North American and European organizations completed our survey. The survey questions are provided in Appendix C. These participants were located primarily in the United States (N = 7), followed by Canada (N = 2), United Kingdom (N = 1), and Zimbabwe (N = 1). Participants were recruited from contact lists the researchers had from prior engagements, as well as requests to CISOs we already knew.

Fear appeal recipient opinions

Our primary research questions were:

RQ1 Did potential cybersecurity fear appeal recipients approve of the use of such fear appeals to motivate secure behaviors?
RQ2 How did cybersecurity fear appeals make potential recipients feel?
RQ3 How did potential cybersecurity fear appeal recipients feel about the ethics of such fear appeals?

Recruitment: recipients

We surveyed 400 workers on a crowdsourcing platform in order to assess their responses to, and feelings about, being targeted by cybersecurity fear appeals (Steelman et al. 2014). Workers were paid $1.50 for completing the survey. Attention questions were embedded in order to weed out inattentive responses, with 3.4% of participants failing one or more of these questions. The mean and median time to complete the survey was 9.77 and 7.07 minutes, respectively. A large majority (94.2%) of participants reported that the time and effort to complete the survey for the compensation received was easier or comparable to other projects. All participants reported being a resident of the United States. The survey questions are enumerated in Appendix D.

Phase 2: Results

Analysis

The transcripts of the interviews and the survey responses were analyzed using thematic analysis, focusing on identifying themes and patterns related to the use of fear appeals in cybersecurity. The authors then met to agree on the final codes. The final codes were then aligned with the three research questions. In this discussion a number of potential detriments will emerge, and labeled *PDi* for later reference.

RQ1 Findings

Researchers The researchers we interviewed were generally supportive of the use of fear appeals. Some did express the need for a roadmap to guide experimentation with fear appeals: *come up with some kind of roadmap for some methodology, some guidelines to ensure that when fear appeals are being used in the Cyber context [..] that they're mindful of... to help mediate whatever is being done in the work*. Others were happy for their ethical review boards to take the responsibility for ensuring that their studies did not cross ethical boundaries. One researcher expressed concern with 'fear appeal fatigue', saying: *People are getting sick of all of it. It's now I'm just wondering whether we might, you know be confronting the same sort of situation with information security as well*. This introduces ***PD9:*** Contributing towards overall fear fatigue. However, the researcher followed this statement with: *I think people still need to see them because it brings back the security into the mindset and I think lots of it*. This suggests that although they have a concern, they still believe that fear appeals are indicated.

CISOs The CISOs were split in terms of approving of the use of fear appeals in their organizations. Four considered the use of fear appeals acceptable, six were against, and one did not express an opinion. It is interesting to note that the three respondents with the most experience (15–20 years, 21–26 years and 11–14 years) all approved of the use of cybersecurity fear appeals in their organizations. One CISO, who approved, said: *Human nature is usually driven by fear to act in a certain way* and another said: *Fear is an excellent motivator*. One disapproving CISO said: *You want your users to be allies not subjects. Allies see they have a stake and a role in protecting the business, subjects avoid contact with those that may castigate them*. Another commented: *Fear is known to paralyze normal decision making and reactions. This infers a deleterious mental load is being subjected on the user via fear appeals. This could be impacting mental health*. Two potential detriments emerge: *PD1* Alienation of non-cyber employees; *PD2* Paralyzing cybersecurity-related decision making.

Summary The researchers were mostly supportive of the use of cybersecurity fear appeals, which is understandable given their research foci. Fewer than half of the CISOs were supportive though.

RQ2 Findings

Researchers One researcher said: *I acknowledge that certain people probably will respond to a fear appeal and others will respond to something else. So for the group that will respond, I think my belief is the benefits probably outweigh the costs*. Another said: *Most of us who are working this area [snip] believe that people should have more precautions and should have their shields up and be more wary and skeptical of phone calls and emails and everything else*. We asked this researcher: Is there anything else you can think of that that might be another candidate for getting people to care?. The researcher answered: *I don't see it. No*. This is not an overwhelming vote of confidence, giving more of a sense that, of the available tools, fear seems to be the best. Yet, given the first part of this comment, the following potential detriment emerges: *PD3* Succeeding with part of society, and putting a disproportional burden on their shoulders

CISOs When asked to rank the efficacy of all the different kinds of techniques they deploy to address cybersecurity

behaviors (on a scale from 1: ineffective to 7:extremely effective), not a single CISO ranked scary messages as maximally efficacious. (The maximum ranking for scary messages was a 4.) This suggests that even the proponents had a feeling that cybersecurity fear appeals might not be the best way to encourage more secure behaviors. The interventions ranked maximally efficacious by the CISOs were: peer support (2), games (2), skill development and training (1), and monitoring and reporting to managers (1). The latter came from one of the people who did *not* support the use of fear appeals. Yet it could be argued that reporting people to their managers is a kind of fear-based intervention. Some CISOs mentioned being under pressure from auditors and concerns about data breaches, which led them to use fear appeals.

Summary The researchers spoke about people needing to take particular security actions, and reasoned that fear appeals motivated them to do this. The CISOs were not as convinced of the efficacy of fear appeals.

RQ3 Findings

Researchers All of the researchers mentioned the need to get IRB approval before carrying out a fear appeal study so that they could ensure that the researcher's planned intervention was ethical. A number of ethical concerns were mentioned by the researchers: the fear appeals being considered manipulative, not causing mental or emotional harm, getting the balance right, and not scaring people unduly. One researcher said: *so there's always like of course you [get] the research benefits in terms of how accurate your research would be and also, on the other hand, how much risk or how much distress that might bring the participants and it's just I guess you kind of have to find a middle ground in there*. One researcher did not consider it unethical to lie: *I would say when the motive is truly to improve the behaviors about what people are doing that it would not be a terrible ethical issue*.

Another researcher, who had over-sold a particular consequence in a fear appeal study, said he would not do so again, because of the unexpected anger and resentment this caused.

The following potential detriments emerge from this discussion: *PD4* Risks being over inflated or untruthful, to maximize motivation to take cybersecurity actions. *PD5* Giving too little added security in return for experienced fear.

One researcher emphasized the need to include a recommended action in the fear appeal: *I would hope as part of a fear appeal study that there is some... mitigation strategy that you are giving them for how to address that fear*

This introduces the next potential detriment: *PD6* People being unable to take cybersecurity actions to assuage the triggered fear.

A number mentioned the need to debrief participants to respect their need to be informed of the intervention and the anticipated outcome: *So really importantly is again the debriefing process at the very end and I think Internet research always nowadays would bring a challenge to this. ...So I think it's just to make sure that there is an elaborate debriefing process even if people drop out of an experiment in the middle.*

This introduces the next potential detriment: *PD7* People being treated as a means to an end, without full information.

Interviewees also emphasize the need for researchers to discuss cybersecurity fear appeal designs with each other. One interviewee said: *...what was actually currently being published in a particular domain or what other researchers are doing* . Another mentioned mentoring his own students designing fear appeal studies: *I know when working with some doc students that are designing their fear appeal studies they're asking a lot of questions about IRB and previous experiences with IRB*. Also mentioned was the value of discussing fear appeal designs at conferences with peers: *I think conversations at conferences like the one we will have at [snip] when researchers can talk about the experiences they've had and the impact their fear appeals have had. So a lot of it based on my previous experiences, but I want to share those with other people when I can. So, conferences are great places to do that. They don't really show up in the papers themselves.*

CISOs The ethical concerns mentioned by the CISOs included being truthful to employees, unintended negative side effects that could bleed into their carrying out their work-related tasks, negative consequences by impacting the cybersecurity program over time, and potential mental health impacts. Some considered lying to employees unethical: *You must be truthful and not spread unnecessary FUD (fear, uncertainty, and doubt)*. CISO2 highlighted the need to give the person some action to take: *Fear is only effective if it is accompanied by a solution to ease that fear. Fear in itself will turn to indifference if not properly directed.*

To illustrate the potentially negative consequences of fear appeals, CISO7 said, of a fear appeal his organization adopted: *It was discontinued after the printouts [reports of undesirable behaviors] dwindled down to nothing, but the damage to the perception of Security lasted long after* (text in square brackets added by authors). He added: ... *also caused or added to a deep distrust and resentment in the security department not only by associates called out in the reports, but peers who thought this was the wrong way to handle the problem*. This supports potential detriments PD1, PD4 & PD6 and introduces: *PD8* Employees becoming disgruntled.

CISO3, asked about testing efficacy of fear appeals, said: *We never specifically measured it. Monthly security drills though seem to produce consistently same results*. This suggests that behavioral interventions are being used in some

Table 1 How respondents felt when shown a cybersecurity fear appeal (multiple responses permitted)

Response	%	Response	%
Uneasy	43.3	Necessary	20.8
Dislike	41.3	Motivating	18.5
Informative	33.3	Retreat	5.8
Uncertain	24.8	Empowering	5.5
Indifferent	23.8		

organizations without any kind of calibration to confirm their efficacy. This supports PD1 and PD5.

Fear appeal recipients' reactions

RQ1 findings

We asked whether our respondents approved of cybersecurity fear appeals. 44.00% approved, 47.50% did not approve and 8.50% said it depended on a number of factors. These 34 responses fell into a number of categories. Some said they would approve if they deemed its use justified. Others were concerned about the negative consequences of the fear appeal on the recipient, one pointing out that the recipient may not have sufficient skills to manage the risk the fear appeal is communicating, supporting PD6. Another said: *Can possibly create anxiety/depression/paranoia depending on the person* introducing *PD10* Creating cybersecurity-related anxiety and paranoia.

A number of respondents said that they did not approve of over-inflating the risk or going "over the top". One said *If it's factual then yes. If it's made up statistics to scare people, then no*, supporting PD4.

Another response said: *Use of fear grabs people's attention and motivates them to do something but I do not care for it*, which indicates that this particular respondent could see why they were used, but did not feel happy about their use. This supports PD7.

RQ2 findings

When offered a list of responses reflecting how people felt when confronted by cybersecurity fear appeals, their responses are shown in Table 1. When asked to choose only *one* response, their responses are depicted in Fig. 5 in the Appendix. The general responses are negative, people mostly indicating uneasiness and dislike for this kind of message. They did not find these messages empowering, even though they are clearly intended as such by their deployers. This introduces a new potential detriment: *PD11* Making people feel uneasy about cybersecurity and causing negative emotions.

Table 2 Cybersecurity fear appeal detriments mentioned by the different stakeholders (Res = Researcher; Org = Organization; Ind = Individual)

		Res	Org	Ind
PD1	Alienation of non-cyber employees		•	
PD2	Paralyzing cybersecurity-related decision making		•	
PD3	Succeeding with cybersecurity skilled members of society, and putting a disproportional burden on their shoulders	•		
PD4	Risks being over inflated or untruthful, to maximize motivation to take cybersecurity actions	•	•	
PD5	Giving too little added security in return for experienced fear	•	•	
PD6	People being unable to take cybersecurity actions to assuage the triggered fear	•	•	•
PD7	People being treated as a means to an end, without full information	•		•
PD8	Employees becoming disgruntled		•	
PD9	Contributing towards overall fear fatigue	•		
PD10	Creating cybersecurity-related anxiety and paranoia			•
PD11	Making people feel uneasy about cybersecurity and causing negative emotions			•

RQ3 findings

When asked how they felt about the questions shown in Fig. 4 (in Appendix), the number of people choosing the response is shown next to the question. Once again, respondents indicated their disapproval and their reservations about the use of cybersecurity fear appeals.

Summary

Table 2 summarizes this discussion, showing which potential detriments were highlighted by each stakeholder group. These feed into the final section where we derive the overarching ethical principles to inform cybersecurity fear appeals.

Phase 3: Deriving ethical principles (Ei)

Table 3 uses the insights gathered from the consultation process to develop the Effects-Reasoning Matrix (ERM) (Duke et al. 1993).

Ethical considerations

A number of ethical requirements emerged from the previous discussion. We will discuss each of these, then provide a brief *precis* of how a snapshot of cybersecurity fear appeal studies have dealt with this ethical consideration. We have not attempted to include each and every study, but rather to use a representative sample of cybersecurity research that has employed fear appeals. The chosen studies were found by using the search terms "fear appeal" and "security" to provide as broad of an initial search criteria as possible, given the varying terms used (e.g., cybersecurity, information security, information systems security, etc.). The initial search was performed using the Business Source Complete research database. Seventeen studies were identified through this search with six not being related to cybersecurity. Two other studies that were related to cybersecurity were not included; one was a review article without a fear appeal deployment, while the other one was not focused on cybersecurity, but rather the economic ramifications of a massive cyber attack. We then used the Academic Search Complete database and found one additional study. Next, we performed the same search using Google Scholar and examined the first 20 results to determine if we were missing a relevant study based on the aforementioned search terms and the ranking algorithm deployed by Google. Four additional studies were identified. Finally, we examined the references of the included studies to this point (i.e., 14) to determine if there were any significant studies that we were missing. A study was considered significant at this stage if it met the previously noted inclusion criteria and had 100 or more citations per Google Scholar. We found three additional studies through this technique. The final number of studies included was 17.

Our final list of studies used fear appeals for: anti-malware software installation (Boss et al. 2015), compliance with security policies (Johnston et al. 2015; Herath and Rao 2009; Johnston and Warkentin 2010; Mwagwabi et al. 2018; Wall and Warkentin 2019; Du et al. 2013), encouraging backups (Boss et al. 2015; Crossler 2010), engendering organizational commitment (Posey et al. 2015), improving organizational security (Warkentin et al. 2016), phish detection (Jansen and van Schaik 2019), warnings about ransomware (Marett et al. 2019), using a PIN on their mobile phones (Albayram et al. 2017), improving online security behavior (van Bavel et al. 2019), discouraging password reuse (Jenkins et al. 2014), improving employee security behavior (Johnston et al. 2019), and improving password selection (Vance et al. 2013).

E1: Obtain IRB approval

The researcher should request and obtain approval from their organization's *Institutional Review Board* (IRB) or equivalent body. While this is an umbrella concept, it can be considered specifically to address potential detriments PD2, PD3, PD6, PD9 and PD10.

Since cybersecurity fear appeal research inherently involves human participation, it is generally a legal or institutional requirement (or both) for the principal investigator to have sought and received approval prior to the involvement of human participants in any study. This type of activity involving ethics has been termed "procedural ethics" by some (Guillemin and Gillam 2004). In its most basic form, it reassures the reviewing body that the researcher can be trusted to perform the research ethically with high regard for participants.

IRBs usually require researchers to ensure that people understand the purpose of the fear appeal and the concomitant risks, and ensure that participants provide *informed consent* before participation (Anabo et al. 2019). Effectively, it ensures that participants retain the right to self-determination and autonomy (Miller and Boulton 2007). In practice, this generally involves giving the participant a written statement explaining the study, its purpose, expected duration, confidentiality and limits, contact information if questions or concerns should arise, compensation that will be provided, potential risks, how these risks relate to those commonly encountered in everyday life, the potential benefits of the study, and reassures the participant that they can cease involvement in the research at any time, and for any reason (American Psychological Association 2016). Informed consent may be waived in some cases, e.g., for anonymous surveys or naturalistic observations (American Psychological Association 2016).

Cybersecurity fear appeal studies In the cybersecurity fear appeal studies we examined,

it was more of an exception than a rule for a study to indicate that informed consent was obtained from research participants, with only the following doing so (Boss et al. 2015; Marett et al. 2019; Vance et al. 2013; van Bavel et al. 2019). However, the description of the methods employed strongly suggested that consent was obtained. For example, Herath and Rao (2009) detailed the steps taken to ensure their participants felt comfortable regarding their anonymity, such as using codes and noting that the data collected was for research purposes only (Herath and Rao 2009).

Table 3 Effects-reasoning matrix (ERM) for cybersecurity fear appeals

	Consequences	Utilitarianism	Kantian	Justice
Researcher	Example Benefit			
	Understanding how better to motivate secure behaviors	Society gains from everyone acting to prevent cybercrime	Individuals need to know about consequences and ameliorations	One person scared into behaving securely reduces the threat for society
	Possible Detriment			
	PD2: Paralyzing cybersecurity-related decision making	PD6: People being unable to take cybersecurity actions to assuage the triggered fear	PD4: Risks being over inflated or untruthful, to maximize motivation to take cybersecurity actions	PD3: Succeeding with cybersecurity skilled members of society, and putting a disproportional burden on their shoulders
Organization	Example Benefit			
	Fewer Cybersecurity Incidents	Less risk of reputational damage	Full disclosure of the purpose of the study	Improve employee resilience
	Possible Detriment			
	PD1: Alienation of employees	PD5: Giving too little added security in return for experienced fear	PD7: People being treated as a means to an end, without full information	PD8: Employees becoming disgruntled
Individual	Example Benefit			
	Heightened cybersecurity awareness	Reduced chance of falling for a cyber attack	Individuals are given accurate and authentic information about risks and mitigations	All members of society, regardless of education and wealth, knowing how to secure their devices
	Possible Detriment			
	PD11: Making people feel uneasy about cybersecurity and causing negative emotions	PD2: Paralyzing decision making	PD10: Creating cybersecurity-related anxiety and paranoia	PD9: Contributing towards overall fear fatigue.

Most institutions require this (Sullivan 2019) so that it is likely that all of these studies did go through the proper IRB process. Not reporting on IRB approval is not unique to cybersecurity (Myles and Tan 2003; Yank and Rennie 2002).

E2: Make cybersecurity benefits salient

It became apparent that there had to be a clear benefit to the cybersecurity fear appeal for people to believe that they were being treated fairly by targeting them with the appeal. This was a concern expressed by both cybersecurity deployers and recipients. Ensuring that we are not using people as a means to an end, and taking cognizance of their need for a benefit, addresses potential detriments PD3, PD5, PD7 and PD8.

It is the responsibility of the researcher to inform the participant of a cybersecurity fear appeal study's risks and potential benefits; this practice has a long history across multiple disciplines (Faden and Beauchamp 1986). In essence, this addresses justice theory's concept of fairness. The person being targeted by the cybersecurity fear appeal has to perceive the *fairness* of the appeal, and of the required cybersecurity-related recommended action. Perceptions of fairness may also lead to greater adherence to the recommended action (Henle et al. 2009).

While this calculus subsumes an inherently utilitarian philosophical perspective (Buchanan and Ess 2008), the consequentialist approach remains the primary means through which a determination is made on the ethical acceptability of a research study involving human participants (Haigh and Jones 2005). Part of this calculus should naturally consider the potential harm a participant may face without the messaging received in a study involving an element of fear.

While this may simply be the opposite side of the same coin, a participant in such a study may not only receive some discernible benefit in terms of improved cybersecurity, but may also avoid a potential harm. For example, a cybersecurity fear appeal study may focus on the dangers associated with ransomware and explain how this may be ameliorated by backing up all data. A participant that receives this messaging may choose to follow the recommended action. However, if the individual did not participate in the cybersecurity fear appeal study, including some of the psychological costs associated with fear induction, the consequences could be much worse. An individual could easily lose all of her important data; a result most would consider much worse than some momentary psychological costs associated with the feeling of fear.

Cybersecurity fear appeal studies It is possible that most (if not all) of the studies included in our analysis did consider how the costs of the study compared to the perceived benefits, but a discussion of these considerations was often not explicitly included in the papers. Given the prevalence of online data collection and the use of the Internet for cybersecurity fear appeal studies, additional considerations may need to inform practice.

E3: Deception must be justified

Some of our deployers considered deception acceptable, while others did not. Individuals also objected to deception and untruthfulness in cybersecurity fear appeals. This suggests the need for deception to be robustly justified before it is used in a cybersecurity fear appeal. Ensuring truthfulness, unless deception is robustly justified, addresses potential detriments PD1, PD4, PD7 and PD10.

While some philosophical perspectives may not find the use of deception ethical in any context, such as Kantian ethics, it is generally regarded as a necessary component of a variety of types of research (Miller et al. 2005). Some fear appeal studies may constitute a straightforward cybersecurity fear appeal without the need for deception (e.g., Johnston et al. 2015), while other studies may use deception to provide a more realistic experimental scenario (e.g., Boss et al. 2015). Although alternatives have been advanced, such as role playing (Holmes and Bennett 1974), the use of deception remains an important research tool. Nonetheless, its use has waned in recent years in some disciplines, such as psychology, as methods, theory, and ethical standards have evolved (Nicks et al. 1997). When deception *is* used, additional justifications must be provided (American Psychological Association 2016).

Cybersecurity fear appeal studies Deception appears to have been used very rarely in the cybersecurity fear appeal studies we examined here with only one reporting its use (Boss et al. 2015). Even studies involving experimental manipulations, or those that attempted to elicit different levels of fear, did not report using deception. For those studies that did not explicitly state whether deception was used, it appears to be because deception was simply not involved in the study protocol rather than failing to indicate one way or the other. Moreover, the lack of deception in cybersecurity fear appeal studies seems to suggest that they may not be a critical element in most contexts. In some type of experimental studies, whether field or laboratory, it might not only make sense, but be necessary to employ some level of deception so that realistic results may be obtained (e.g., Boss et al. 2015). It is also possible that cybersecurity researchers may continue to seek other ways in which equivalent results may be obtained, similar to other disciplines (Nicks et al. 1997). This may not eliminate the use of deception, but may serve to minimize it.

E4: Provide feasible recommended cybersecurity action

Both cybersecurity fear appeal deployers and targets mentioned that a recommended action ought be provided to ensure that people can assuage their fear (Renaud and Dupuis 2019).

The recommended action gives the participant a reasonable cybersecurity action that can be taken, thereby making it possible for the recipient to engage in danger control (Lawson et al. 2016; Leventhal 1970; Witte 1992). Ensuring that a *feasible* action is available addresses potential detriment PD6.

A recommended cybersecurity action is more likely to be seen in experimental research involving a treatment of some kind since what one would generally test for is the degree to which the recommended action has been used (e.g., Davinson and Sillence 2010). From an ethical standpoint, a recommended cybersecurity action should be advised when an explicit fear appeal is used. In other words, if you are going to elicit fear then you should provide information on how to assuage that fear, some feasible cybersecurity action to take, as this is a major and essential component of a fear appeal (Mwagwabi et al. 2018).

A recommended action may be included as part of the fear appeal messaging only, and not included in messages delivered to the control group or separate treatment group. However, this may result in the control group (or another treatment group in the case of a modified classical design) not receiving information on the recommended action, which could well obfuscate the primary reason for differences in behaviors between experimental groups, not the influence of the fear itself. Given the central role a recommended action may play in the development of adequate levels of self- and response-efficacy (Witte 1996), it is possible the lack of adoption is related to recipients not knowing about the recommended action, rather than the absence of fear. Considering the central role self-efficacy has had in behavioral outcomes in protection motivation theory studies (Floyd et al. 2000; Milne et al. 2000), it is important that this is taken into account.

The ethical concerns related to inducing fear may become a moot point if, in reality, it is information on the recommended action that is effectuating a positive change and not the induction of fear itself. While it is unlikely to be attributable fully to one or the other, and may vary based on context, the level of ambiguity remains a concern (De Hoog et al. 2007, 2005). Thus, it is difficult to know, with any reasonable level of assurance, until studies begin consistently empirically testing for this within the cybersecurity domain. However, there is ample evidence that suggests the recommended action component of a fear appeal is effective (Ruiter et al. 2014). Not controlling for the effect of the recommended action constitutes an important opportunity being missed, both from an ethical standpoint and more broadly speaking as well.

Cybersecurity fear appeal studies Most of the fear appeal studies we examined did include a recommended action (Boss et al. 2015; Johnston et al. 2015; Johnston and Warkentin 2010; Jansen and van Schaik 2019; Albayram et al. 2017; Marett et al. 2019; Mwagwabi et al. 2018; Jenkins et al. 2014; Wall and Warkentin 2019; Johnston et al. 2019; Du et al. 2013; van Bavel et al. 2019). Given the central importance of providing a recommended action in the wake of a fear appeal, this is encouraging. It is possible that the other studies did provide a recommended action, but did not explicitly report on it. In some disciplines a recommended action may be self-evident, such as anti-smoking campaigns. However, even then we see explicit recommended actions being provided to the individual (i.e., quitting smoking) (Leventhal and Watts 1966). Given the abstract nature of cybersecurity from the perspective of the target audience (West 2008), what may be self-evident to the researcher may not be entirely clear to the intended recipients.

E5: Calibrate during deployment

The experiences of one of the researchers and one of the CISOs with fear appeals that overstepped the mark, suggests the need for calibration to take place, before and during deployment to monitor the success of the intervention and to uncover potential negative side effects. Calibration addresses potential detriments PD1 and PD4.

Because fear appeals aim to make people feel fearful, it is essential that the fear appeal deployer: (1) designs the cybersecurity fear appeal with great care, and, if the decision to deploy is made, (2) carefully monitors the deployment at regular intervals. This is even more important for cybersecurity appeals, than for fear appeals in more established domains, because the general population often do not have high levels of cybersecurity expertise and a poorly designed fear appeal could make them overly fearful.

In terms of design, many of our fear appeal researcher interviewees mentioned consulting with their peers when designing a fear appeal.

In terms of monitoring, it is advisable to measure levels of elicited fear, potential negative consequences, and feasibility of the recommended action for the targeted recipients (Renaud and Dupuis 2019). The option to call a halt to the experiment/deployment should always be on the table.

Calibration ought to be carried out in the spirit of Kant's golden rule, as argued by one of our interviewees: *I generally like to view everything I do from the perspective of the golden rule, which says do unto others as you would have them do unto you so when you put yourself in that perspective of your participants*.

Cybersecurity fear appeal studies Based on our interviews with researchers, calibration from an ethics standpoint may be done in some contexts in cybersecurity fear appeal studies. However, it is not something commonly reported on in the studies we examined. The informal discussions that may take place at conferences and between faculty and students are important, but do not replace results that could be obtained from a more formalized calibration process. Normative concepts, such as ethics, may benefit from a calibration process (Uviller 2000) and should be considered and reported on in all fear appeal studies, and this includes those used in the cybersecurity domain.

E6: Debrief at conclusion of experiment

A number of researchers highlighted the need for cybersecurity fear appeal recipients to be debriefed at the conclusion of an experiment. Giving people due respect by debriefing them addresses potential detriments PD1 and PD7.

Debriefing involves a communication with the participants at the conclusion of a research study, with information generally provided about the true nature of the study (Smith and Richardson 1983).

The debrief serves multiple purposes, including providing a venue for participants who may have felt harmed in some way to discuss the matter with the researcher. In these particular cases, debriefing has been found to be a powerful tool in mitigating the harm that may unintentionally have been caused (Smith and Richardson 1983).

In some studies, a formal debriefing may not be practical, such as a large-scale survey with anonymous participants. However, even in these kinds of studies, it is possible to provide participants with the option of being able to read the resulting research report (e.g., website address that they may check at a later date).

While debriefing is important, in some instances it may be omitted if there are scientific merits to doing so and the potential risks to the participants are minimal (American Psychological Association 2016).

Cybersecurity fear appeal studies Debriefing is not reported in most of the cybersecurity fear appeal studies we analyzed, the exception being (Boss et al. 2015). This may be partly due to the changing nature of research in which a large proportion of studies are conducted online rather than in-person (Kraut et al. 2004). However, even when this is the case, debriefing of some type should still occur unless there are clear justifications for its omission.

Summary

Figure 3 depicts the ethical principles and Table 4 shows how these ethical principles address the perceived detriments that emerged from our consultation.

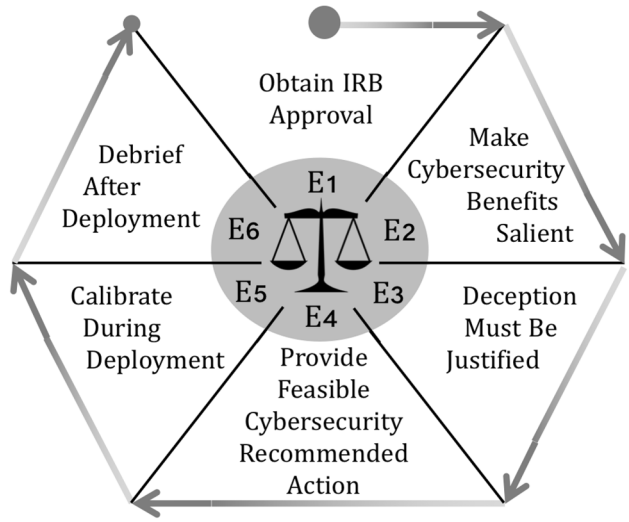


Fig. 3 Cybersecurity fear appeal ethical principles for informing their design and deployment

Reflection

In experimenting with fear appeals in cybersecurity, researchers seek to determine whether it is possible to transfer an intervention that has, up to now, performed with efficacy in the safety context (e.g. health (Witte et al. 2001) and personal care (Bartikowski et al. 2019)) to the cybersecurity context (something that can harm your devices and might harm you in a very small percentage of cases). The kinds of system where a lack of cybersecurity can cause *physical* harm are referred to as "cyber-physical" systems [110]. Yet, it must be acknowledged that a failure of cybersecurity could also lead to psychological harm, especially when fear appeals are deployed. This might be the case when the person being targeted is already anxious about other things, or does not feel competent to take the recommended action. This was the rationale for the research reported in this paper.

In this paper, we report on how we derived a set of cybersecurity-specific ethical principles to inform the deployment of cybersecurity fear appeals.

We commenced with an overview of the components of fear appeals (*FAi*), and a discussion of the three ethical theories that could be used to contemplate the impacts of their deployment. We then interviewed cybersecurity fear appeal deployers and recipients to derive a set of potential detriments related to their deployment, specifically in the cybersecurity domain (*PDi*).

Our investigation suggests that cybersecurity fear appeals ought to be used with caution. To exercise such caution, we ought first to ensure that the

cybersecurity ethical principles we derived inform the design and deployment of cybersecurity fear appeals. Kant's Golden Rule ought to be our guide when deciding on how

Table 4 Mapping the ethical principles (*Ei*) to the perceived detriments (*PDi* - Table 2) and Fear Appeal Components: *FT* fear trigger (FA1), *RE* response efficacy (FA2), *RA* recommended action (FA3), *SE* self-efficacy (FA4) (Section FA4)

		IRB	Benefits	Justified deception	Action	Calibrate	Debrief
		E1	E2	E3	E4	E5	E6
PD1	Alienation of employees			•		•	•
PD2	Paralyzing cybersecurity-related decision making	•					
PD3	Succeeding with cybersecurity skilled members of society, and putting a disproportional burden on their shoulders	•	•				
PD4	Risks being over inflated or untruthful, to maximize motivation to take cybersecurity actions			•		•	
PD5	Giving too little added security in return for experienced fear		•				
PD6	People, being unable to take cybersecurity actions to assuage the fear	•			•		
PD7	People, being treated as a means to an end, without full information		•	•			•
PD8	Employees becoming disgruntled		•				
PD9	Contributing towards overall fear fatigue	•					
PD10	Creating cybersecurity-related anxiety and paranoia	•		•			
PD11	Making people feel uneasy about cybersecurity and causing negative emotions					•	
Fear Appeal Components		All	RE	FT	RA	FT SE	FT

much fear to elicit, while Utilitarianism ought to require us to assure, by constant monitoring during the course of the deployment, that the cybersecurity fear appeal is indeed delivering value. Finally, justice theory considerations highlight the need for participants to feel that they are being treated fairly. It is not enough for us, as researchers, to be able to gain something from the study: participants should be happy to give us the right to target them with cybersecurity fear appeals.

Limitations

The number of cybersecurity fear appeal researchers we interviewed is small. A larger number of interviewees would give a more nuanced insight into their motivations and understandings of the ethical implications of fear appeals. The number of CISOs, too, was relatively small. Widening the sample would be a fruitful avenue for future research.

Therefore, generalizability is inherently limited in this respect. While the insight gained from both sets of research participants varied within the groups and between them, there may be other important insights that could be gained from other CISOs and researchers whose views were not represented here. Likewise, the large-scale survey consisted of participants from the United States only. To the extent that workers on a crowdsourcing platform are generalizable to the population, this population may be limited to people in the United States, given varying cultural norms and customs.

Common method bias is another possible limitation. While common method bias is less likely to be an issue with the data collected on the CISOs and researchers, it can be an issue for the recipients of fear appeals given that a single quantitative methodology was used in a large-scale survey (Podsakoff et al. 2003; Malhotra et al. 2006). However, this was mitigated in part by the use of a participant pool that is able to remain anonymous to the research team; this reduces the likelihood of satificing. Additionally, quality control (i.e., attention check) questions were embedded throughout the survey, as well as non-Likert questions. All of this helps reduce the likelihood that common method bias had a significant role in the results obtained and conclusions made thereof (MacKenzie and Podsakoff 2012).

Conclusion

Cybersecurity researchers carry out research into the use of cybersecurity fear appeals to encourage people to engage in precautionary behaviors or to cease insecure behaviors. CISOs sometimes deploy such appeals in their organizations. In this paper, we explored the ethical issues related to the deployment of fear appeals in the cybersecurity context. By consulting cybersecurity fear appeal deployers and targets we were able to derive a set of six cybersecurity-specific

ethical principles which could guide deployment of such appeals. Our purpose, in writing this paper, is to launch a wider discourse into the ethics related to the deployment of fear appeals in the cybersecurity domain.

Appendix A: Figures

See Figs. 4 and 5.

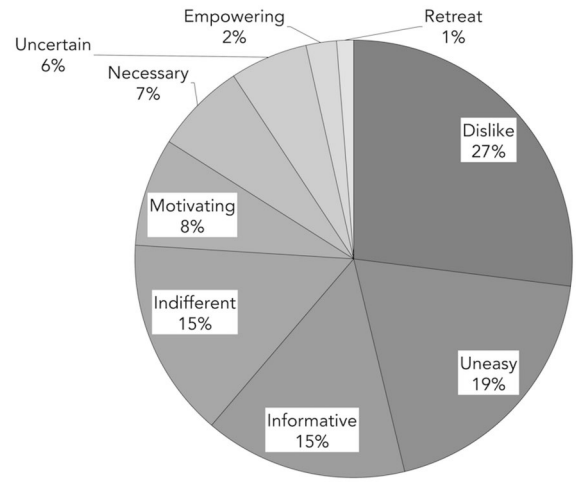


Fig. 5 When asked to choose only one response to the use of cybersecurity fear appeals

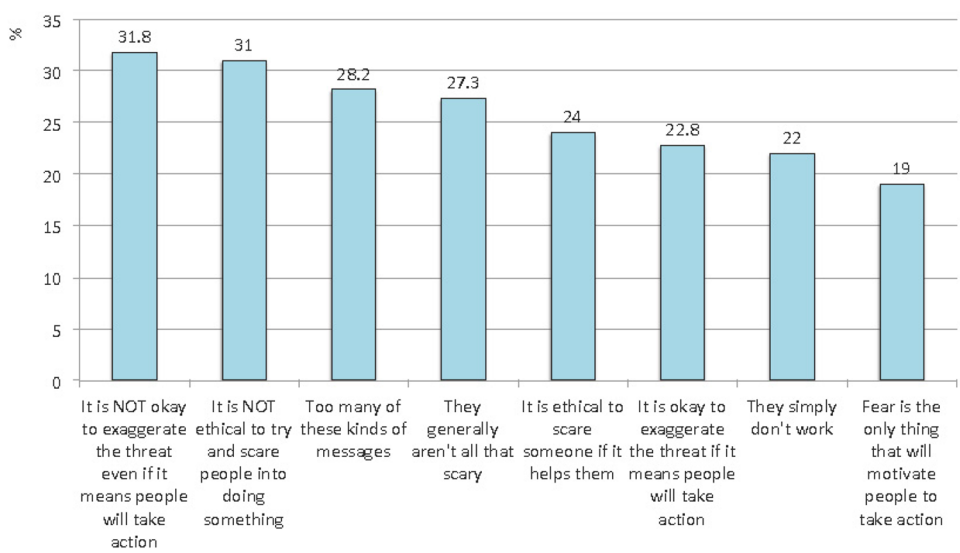


Fig. 4 Percentage of respondents who thought the statement applied to the use of cybersecurity fear appeals (multiple choices permitted)

Appendix B: Interview questions for researchers

(1) In your opinion, what are the primary ethical considerations that a fear researcher should be concerned about?
(2) How do you balance these concerns with the benefits you believe derive from the use of fear appeals?
(3) How do ethical concerns influence the design of fear appeals?
(4) How do ethical concerns influence the deployment of fear appeals?
(5) How do you think fear appeal researchers could improve their consideration of ethical concerns of the use of fear appeals in information security?

Appendix C: Survey questions for CISOs

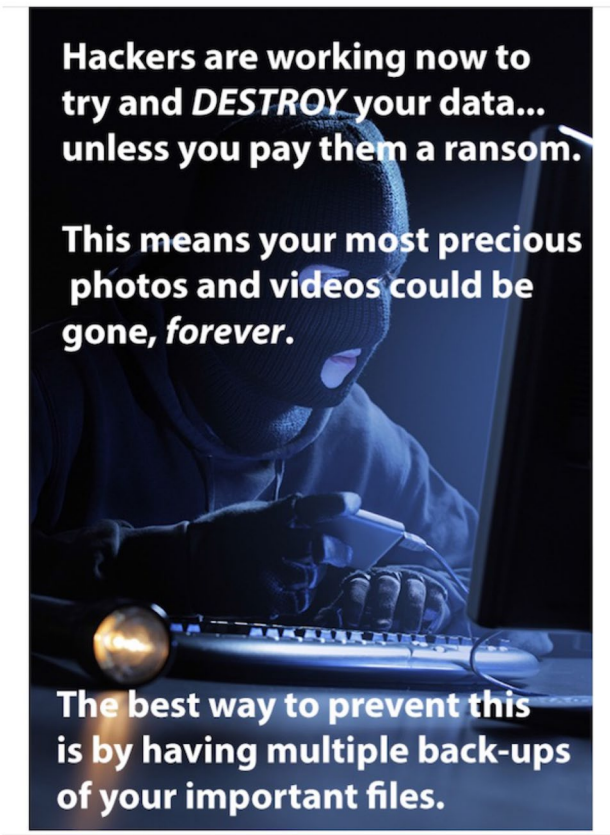
(1) What types of techniques do you deploy in your capacity as CISO: (check as many as you like: awareness campaigns; skill development and training; rewards; scary messages; monitoring and reporting to managers; games; peer support; maintain an information security knowledge repository. [order randomized]
(2) For each of the ones you checked, can you say how effective they are on a scale from 1 (not at all) to 7 (very effective).

A fear appeal is a message that attempts to persuade people to behave securely by scaring them, either by telling them about the consequences of being hacked, or by threatening sanctions within the organization.

(3) In your opinion, are there any ethical considerations that a CISO should be concerned about when using a fear appeal in their organization?
(4) In your opinion, are there any benefits to be gained from using a fear appeal in your organization?
(5) Do you believe that you can balance the ethical concerns with the benefits you can derive from the use of fear appeals?
    (a) for what particular behaviors would a fear appeal be your first option: phishing; locking computer; not plugging in foreign USBs; strong passwords; adopting 2FA. [order randomized]
(6) Do ethical concerns influence whether you decide to use a fear appeal or not in your organization?
(7) Who would have to approve the use of a fear appeal in your organization?
(8) If you've used a fear appeal in the past: tell us about it; how did you determine whether it was effective or not?; did you continue or discontinue using it?
(9) any other thoughts about fear appeals would be welcomed.
(10) Demographics: size of organization, and how long they have been a CISO

Survey questions for recipients

(1) Demographics
(2) Show an image of a cybersecurity fear appeal.



(3) Which of the words below describe how you FEEL about these kinds of messages, ones that try to scare you into taking an action? (choose all that apply): 'Dislike'; 'Informative'; 'Uneasy'; 'Empowering'; 'Motivating'; 'Uncertain'; 'Necessary'; 'Retreat'; 'Indifferent'. [order randomized]
(4) With the same words as the previous question: Which of the words below BEST describes how you FEEL about these kinds of messages, ones that try to scare you into taking an action? (select your top one only)
(5) The message we show above attempts to make people feel afraid. Do you approve of the use of fear in cybersecurity messages? 'yes', 'no', and 'it depends' (please explain)

(6) Which of the options below describe what you THINK about these kinds of messages, ones that try to scare people into taking an action? (choose all that apply): "They simply don't work"; "It is ethical to scare someone if it helps them"; "It is okay to exaggerate the threat if it means people will take action"; "It is NOT okay to exaggerate the threat even if it means people will take action"; "It is NOT ethical to scare someone into doing something"; " They generally aren't that scary"; "Too many of these kinds of messages." [order randomized]

References

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T., & Upton, D.M. Cyber harm: Concepts, taxonomy and measurement, Saïd Business School WP 23.

Albarracín, D., Gillette, J. C., Earl, A. N., Glasman, L. R., Durantini, M. R., & Ho, M.-H. (2005). A test of major assumptions about behaviorchange: 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.

Albayram, Y., Khan, M.M.H., Jensen, T., & Nguyen, N. (2017). "... 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), Santa Clara, CA (pp. 49–63).

American Psychological Association, Ethical Principles of Psychologists and Code of Conduct. Retrieved May 18, 2018, from http://www.apa.org/ethics/code/index.aspx.

Anabo, I. F., Elexpuru-Albizuri, I., & Villardón-Gallego, L. (2019). Revisiting the belmont report's ethical principles in internet-mediated research: Perspectives from disciplinary associations in the social sciences. *Ethics and Information Technology*, *21*(2), 137–149.

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

Arthur, D., & Quester, P. (2003). The ethicality of using fear for social advertising. *Australasian Marketing Journal (AMJ)*, *11*(1), 12–27.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, *52*(1), 1–26.

Bartikowski, B., Laroche, M., & Richard, M.-O. (2019). A content analysis of fear appeal advertising in Canada, China, and France. *Journal of Business Research*, *103*, 232–239.

Bayer, R., & Fairchild, A. L. (2016). Means, ends and the ethics of fear-based public health campaigns. *Journal of Medical Ethics*, *42*(6), 391–396.

Beck, K. H. (1984). 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.

Benet, S., Pitts, R. E., & LaTour, M. (1993). The appropriateness of fear appeal use for health care marketing to the elderly: Is it OK to scare Granny? *Journal of Business Ethics*, *12*(1), 45–55. https://doi.org/10.1007/BF01845786.

Berelson, B., & Steiner, G. A. (1964). *Human behavior: An inventory of scientific findings*. Harcourt: Brace & World.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–64.

Brennan, L., & Binney, W. (2010). Fear, guilt, and shame appeals in social marketing. *Journal of Business Research*, *63*(2), 140–146.

Buchanan, E., & Ess, C. (2008). *Internet research ethics: The field and its critical issues*. Hoboken: Wiley.

Capurro, R., & Pingel, C. (2002). Ethical issues of online communication research. *Ethics and Information Technology*, *4*(3), 189–194.

Cavanagh, G. F., Moberg, D. J., & Velasquez, M. (1981). The ethics of organizational politics. *Academy of Management Review*, *6*(3), 363–374.

Chen, M.-F. (2016). Impact of fear appeals on pro-environmental behavior and crucial determinants. *International Journal of Advertising*, *35*(1), 74–92.

Cowan, R. (1986). How the narcs created crack. *National Review*, *38*, 26–31.

Crossler, R.E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. In: Proceedings of the 43rd Hawai'i International Conference on System Sciences, IEEE, Honolulu, HI, USA. https://ieeexplore.ieee.org/abstract/document/5428416

Dabbs, J. M, Jr., & Leventhal, H. (1966). Effects of varying the recommendations in a fear-arousing communication. *Journal of Personality and Social Psychology*, *4*(5), 525–531.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among Internet users. *Computers in Human Behavior*, *26*(6), 1739–1747.

De Hoog, N., Stroebe, W., & De Wit, J. B. (2005). The impact of fear appeals on processing and acceptance of action recommendations. *Personality and Social Psychology Bulletin*, *31*(1), 24–33.

De Hoog, N., Stroebe, W., & De Wit, J. (2007). 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.

Dillard, J. P. (1994). Rethinking the study of fear appeals: An emotional perspective. *Communication Theory*, *4*(4), 295–323.

Dillard, J. P., Li, R., Meczkowski, E., Yang, C., & Shen, L. (2017). Fear responses to threat appeals: Functional form, methodological considerations, and correspondence between static and dynamic data. *Communication Research*, *44*(7), 997–1018.

Du, H., Xu, H., Rosson, M.B., & Carroll, J.M. (2013). Effects of Fear appeals and point of reference on the persuasiveness of IT security communications. In: IEEE international conference on intelligence and security informatics, IEEE, 2013, pp. 82–84.

Duke, C. R., Pickett, G. M., Carlson, L., & Grove, S. J. (1993). A method for evaluating the ethics of fear appeals. *Journal of Public Policy & Marketing*, *12*(1), 120–129.

Emery, S., Szczypka, G., Abril, E., Kim, Y., & Vera, L. (2014). Are you scared yet? Evaluating fear appeal messages in tweets about the tips campaign. *Journal of Communication*, *64*(2), 278–295.

Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. New York: Oxford University Press.

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

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

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

Furedi, F. (2018). *How fear works: Culture of fear in the twenty-first century*. London: Bloomsbury Publishing.

Graham, C. (2019). The United States Prohibition of Alcohol. Rtrieved September 14, 2019, fromhttps://www.cato.org/publications/policy-analysis/alcohol-prohibition-was-failure.

Guillemin, M., & Gillam, L. (2004). Ethics, reflexivity, and "ethically important moments" in research. *Qualitative Inquiry*, *10*(2), 261–280.

Haigh, C., & Jones, N. A. (2005). An overview of the ethics of cyber-space research and the implication for nurse educators. *Nurse Education Today*, *25*(1), 3–8. https://doi.org/10.1016/j.nedt.2004.09.003.

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

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

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

Henle, C. A., Kohut, G., & Booth, R. (2009). Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory. *Computers in Human Behavior*, *25*(4), 902–910.

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

Holmes, D. S., & Bennett, D. H. (1974). Experiments to answer questions raised by the use of deceptionin psychological research: I. Role playing as an alternative to deception; II. Effectiveness of debriefing after a deception; III. Effect of informed consent on deception. *Journal of Personality and Social Psychology*, *29*(3), 358–367.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion*. London: Yale University Press.

Hyman, M. R., & Tansey, R. (1990). The ethics of psychoactive ads. *Journal of Business Ethics*, *9*(2), 105–114.

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

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). 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.

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

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

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

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

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

Kraut, R., Olson, J., Banaji, M., Bruckman, A., Cohen, J., & Couper, M. (2004). Psychological research online: Report of Board of Scientific Affairs' Advisory Group on the Conduct of Research on the Internet. *American Psychologist*, *59*(2), 105–117.

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

Lau, J., Lee, A., Wai, S., Mo, P., Fong, F., Wang, Z., et al. (2016). 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.

Lawson, S.T., Yeo, S.K., Yu, H., & Greene, E. (2016). 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, NATO CCO COE Publications, Tallinn, Estonia (pp. 65–80). https://doi.org/10.1109/CYCON.2016.7529427. https://ieeexplore.ieee.org/abstract/document/7529427

Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. E. Berkowitz & E. E. Walster (Eds.), *Advances in experimental social psychology* (pp. 119–186). Amsterdam: Elsevier.

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

Lewis, I., Watson, B., & White, K. M. (2008). 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.

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of Retailing*, *88*(4), 542–555.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in is research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865–1883. https://doi.org/10.2307/20110660.

Marett, K., Vedadi, A., & Durcikova, A. (2019). A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses. *Computers & Security*, *80*, 25–35. https://doi.org/10.1016/j.cose.2018.09.004.

Micewski, E. R., & Troy, C. (2007). Business ethics-deontologically revisited. *Journal of Business Ethics*, *72*(1), 17–25.

Miller, T., & Boulton, M. (2007). Changing constructions of informed consent: Qualitative research and complex social worlds. *Social Science & Medicine*, *65*(11), 2199–2211.

Miller, F. G., Wendler, D., & Swartzman, L. C. (2005). Deception in research on the placebo effect. *PLoS Medicine*, *2*(9), 0853–0859.

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

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Minichiello, V., Rahman, S., Hawkes, G., & Pitts, M. (2012). STI epidemiology in the global older population: Emerging challenges. *Perspectives in Public Health*, *132*(4), 178–181.

Moore, M.H. (1989). Actually, prohibition was a success, the New York Times. Retrieved September 14, 2019, from https://www.nytimes.com/1989/10/16/opinion/actually-prohibition-was-a-success.html.

Mwagwabi, F., McGill, T. J., & Dixon, M. (2018). 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. https://doi.org/10.17705/1CAIS.04207.

Myles, P. S., & Tan, N. (2003). Reporting of ethical approval and informed consent in clinical research published in leading anesthesia journals. *Anesthesiology: The Journal of the American Society of Anesthesiologists*, *99*(5), 1209–1213.

Nicks, S. D., Korn, J. H., & Mainieri, T. (1997). The rise and fall of deception in social psychology and personality research, 1921 to 1994. *Ethics & Behavior*, *7*(1), 69–77.

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

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

Peters, G.-J. Y., Ruiter, R. A. C., & Kok, G. (2014). 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.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

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

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

Rawls, J. (2005). *A theory of justice* (reissue ed.). Cambridge: Harvard University Press.

Renaud, K., & Dupuis, M. (2019). Cyber security fear appeals: Unexpectedly complicated. In: New Security Paradigms Workshop, San Carlos, Costa Rica (pp. 42–56), 23–26 September.

Reynolds, S. J., & Bowie, N. E. (2004). A Kantian perspective on the characteristics of ethics programs. *Business Ethics Quarterly*, *14*(2), 275–292.

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

Rogers, R. W., & Mewborn, C. R. (1976). 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.

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, *20*(2), 127–142.

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

Smith, S. S., & Richardson, D. (1983). Amelioration of deception and harm in psychological research: The important role of debriefing. *Journal of Personality and Social Psychology*, *44*(5), 1075–1082.

Stainback, R. D., & Rogers, R. W. (1983). 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.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, *38*(2), 355–378.

Sullivan, G.M. IRB 101, The Accreditation Council for Graduate Medical Education Suite, Chicago, IL, 2011. Retrieved June 6, 2019, from https://relationshipscience.com/organization/accreditation-council-for-graduate-medical-education-786044.

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., et al. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178–1204.

Tengland, P.-A. (2012). Behavior change or empowerment: On the ethics of health-promotion strategies. *Public Health Ethics*, *5*(2), 140–153.

Thompson, P. B. (2012). Ethics and risk communication. *Science Communication*, *34*(5), 618–641.

Tunner, J. F, Jr., Day, E., & Crask, M. R. (1989). Protection motivation theory: An extension of fear appeals theory in communication. *Journal of Business Research*, *19*(4), 267–276.

Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, L., Cranor, L.F., Dixon, H., Emami Naeini, P., & Habib, H., et al.: Design and evaluation of a data-driven password meter. In: Proceedings of the CHI conference on human factors in computing systems, ACM, Denver, CO, 2017, pp. 3775–3786.

Uviller, H. R. (2000). Ethics in criminal advocacy, symposium, the neutral prosecutor: The obligation of dispassion in a passionate pursuit. *Fordham Law Review*, *68*(5), 1695–1718.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003.

Vance, A., Eargle, D., Ouimet, K., & Straub, D.: Enhancing password security through interactive fear appeals: A web-based field experiment, in: 46th Hawai'i International Conference on System Sciences (HICSS), Hawai'i, USA, 2013, pp. 2988–2997.

Wall, J. D., & Warkentin, M. (2019). Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics. *Information & Management*, *56*(8), 103157. https://doi.org/10.1016/j.im.2019.03.002.

Walton, D. (2010). Why fallacies appear to be better arguments than they are. *Informal Logic*, *30*(2), 159–184.

Warkentin, M., Walden, E., Johnston, A., & Straub, D. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194–215.

Watney, S. (1989). Taking liberties: An introduction. In E. Carter & S. Watney (Eds.), *Taking liberties: AIDS and cultural politics* (pp. 11–57). London: Serpent's Tail.

West, H. R. (2004). *An introduction to Mill's utilitarian ethics*. Cambridge: Cambridge University Press.

West, R. (2008). The Psychology of Security. *Communications of the ACM*, *51*(4), 34–40.

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

Witte, K. (1996). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In P. A. Andersen & L. K. Guerrero (Eds.), *Handbook of communication and emotion* (pp. 423–450). Amsterdam: Elsevier.

Witte, K., Meyer, G., & Martell, D. (2001). *Effective health risk messages: A step-by-step guide*. Thousand Oaks: Sage.

Wojciechowski, Ł. P., & Babjaková, V. (2015). Necromarketing in the media and marketing communications. *Social Communication*, *2*(2), 15–29. https://doi.org/10.1515/sc-2015-0007.

Yank, V., & Rennie, D. (2002). Reporting of informed consent and ethics committee approval in clinical trials. *The Journal of the American Medical Association*, *287*(21), 2835–2838.