International Journal of Human-Computer Studies 123 (2019) 40–55

Contents lists available at ScienceDirect

International Journal of Human-Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

The design and evaluation of a theory-based intervention to promote security behaviour against phishing

Jurjen Jansen[a,b,*], Paul van Schaik[c]

[a] Faculty of Humanities & Law, Open University, Heerlen, The Netherlands
[b] Cybersafety Research Group, NHL Stenden University of Applied Sciences & Dutch Police Academy, P.O. Box 1080, Leeuwarden 8900 CB, The Netherlands
[c] School of Social Sciences, Humanities & Law, Teesside University, Borough Road, Middlesbrough TS5 8NQ, United Kingdom

ARTICLE INFO

Keywords:
Information security behaviour
Protection motivation theory
Fear appeals
Intervention
Phishing
Online information-sharing behaviour

ABSTRACT

This study examined the impact of fear appeal messages on user cognitions, attitudes, behavioural attentions and precautionary behaviour regarding online information-sharing to protect against the threat of phishing attacks. A pre-test post-test design was used in which 768 Internet users filled out an online questionnaire. Participants were grouped in one of three fear appeal conditions: strong-fear appeal, weak-fear appeal and control condition. Claims regarding vulnerability of phishing attacks and claims concerning response efficacy of protective online information-sharing behaviour were manipulated in the fear appeal messages. The study demonstrates positive effects of fear appeals on heightening end-users' cognitions, attitudes and behavioural intentions. However, future studies are needed to determine how subsequent security behaviour can be promoted, as the effects on this crucial aspect were not directly observed. Nonetheless, we conclude that fear appeals have great potential to promote security behaviour by making end users aware of threats and simultaneously providing behavioural advice on how to mitigate these threats.

1. Introduction

End-users' information security practices play an essential role in mitigating threats such as phishing scams, malicious software, and distributed denial-of-service attacks within modern, networked society. As more services are offered online and personal data are increasingly stored by digital means, people become more technology-dependent, but also more susceptible to security incidents (Furnell et al., 2007). Precautionary online behaviour by end users is important in safeguarding the online domain, because they play a central role in achieving online security (Davinson and Sillence, 2014; Liang and Xue, 2010; Ng et al., 2009). This study investigates to what extent fear appeals can persuade end users to perform safe online behaviour. Attention to fear and fear appeals is currently lacking in the information security domain (Johnston et al., 2015), but is gaining in popularity (Wall and Buche, 2017). Moreover, as stated by Briggs et al. (2016), the work on behaviour change interventions for cybersecurity is just getting started.

Michie et al. (2011, p. 2) define behaviour change interventions as "coordinated sets of activities designed to change specified behaviour patterns". Interventions aimed at behavioural change are quite common in human-computer interaction studies, but less common in the field of information security (Coventry et al., 2014). However, persuading end users to adequately cope with cyber-threats is not an easy task. Fransen et al. (2015) noted that persuasion plays a prominent role in everyday life, but persuasion efforts in themselves often have limited impact. They suggested that perhaps the most important reason for this is that individuals do not want to be influenced. Another potential reason is that people normally strive to reduce (mental) effort by relying on fast information-processing ("System 1") rather than on deliberate processing ("System 2") (Kahneman, 2011).

This study focusses on protection against a specific online threat, namely phishing attacks, the process of retrieving personal information using deception through impersonation (Lastdrager, 2014). Phishing is considered dangerous to end users (Arachchilage et al., 2016; Arachchilage and Love, 2014; Hong, 2012; Kirlappos and Sasse, 2012) and forms a world-wide problem (APWG, 2018) for different sectors, such as the online payment sector and financial institutions. For online banking for instance, it seems that everyone is susceptible to phishing to some degree (Jansen and Leukfeldt, 2015). However, Purkait (2012, p. 406) argued that "an educated, informed and alert customer could play an important role in improving online banking security and be

* Corresponding author at: Cybersafety Research Group, NHL Stenden University of Applied Sciences & Dutch Police Academy, P.O. Box 1080, Leeuwarden 8900 CB, The Netherlands.
E-mail addresses: j.jansen@nhl.nl (J. Jansen), p.van-schaik@tees.ac.uk (P. van Schaik).

https://doi.org/10.1016/j.ijhcs.2018.10.004
Received 31 January 2018; Received in revised form 14 September 2018; Accepted 25 October 2018
Available online 26 October 2018
1071-5819/

better prepared against phishing attacks.". Phishing attacks do not only target desktop computer users, but also people who are using mobile devices (Goel and Jain, 2018). In these cases, perpetrators do not only use fake e-mail and websites, but also SMS and mobile applications to attack users. In the first quarter of 2018, the Anti Phishing Working Group received some 80,000 unique phishing mail reports by its customers per month (APWG, 2018).

Roughly four different types of intervention can be distinguished in promoting precautionary online behaviour by end users: security education, training, awareness-raising and design (Kirlappos and Sasse, 2012; Posey et al., 2015; Van Schaik et al., 2017). Education involves developing knowledge and understanding of online threats and ways to mitigate threats, while training typically involves developing skills in information security. The aim of increased knowledge and skills is that they transfer to adequate levels of precautionary online behaviour (Van Schaik et al., 2017). Awareness-raising is involved with agenda-setting – or warning users – and focusses attention on threats and countermeasures. Effective security design should facilitate desirable user behaviour (Sasse et al., 2001). Design includes nudges in the environment that gently push an end user, without too much mental effort, to perform the right behaviour (Coventry et al., 2014; French, 2011; Thaler and Sunstein, 2009), for instance by manipulating a default setting to protect user data (Briggs et al., 2016) or placing stickers with information security messages on devices (see e.g., https://www.cpni.gov.uk/workplace-behaviours).

Technical and legal solutions to combat phishing have been proposed as well (Purkait, 2012). Recent examples are "Draw" (Yang et al., 2017), which informs users when phishing conditions are likely to be satisfied, based on traffic rankings of domains, and a two-level authentication approach by Jain and Gupta (2017), which can detect phishing based on search engine and hyperlink information. However, both still require actions by its users. Other examples of technical solutions include automated phishing tools, e-mail filters, and blacklists (Arachchilage and Love, 2014; Corona et al., 2017; Hong, 2012; Ludl et al., 2007), but these solutions provide certain drawbacks, such as false positives, false negatives, and usability issues (e.g., Jain and Gupta, 2017). In addition, safety cues tend to be ignored by end-users (Dhamija et al., 2006) and are also quite easy to manipulate by hackers (Downs et al., 2006). An eye-tracking experiment by Alsharnouby et al. (2015) showed that their participants spend only 6% of the time looking at security indicators and 85% at the content of the webpage when deciding whether a website is legitimate or not. Other research also demonstrated that end users are more focussed on looking for signs that demonstrate trustworthiness than signs that prove security (Kirlappos and Sasse, 2012). In conclusion, technology alone cannot provide the complete security solution; human aspects are essential to address (Furnell and Clarke, 2012).

Although interventions are deemed important, the effectiveness of interventions is yet to be determined. In this study, we focus on a combination of security education and awareness-raising, an approach which finds support from current literature on phishing (Arachchilage and Love, 2014; Downs et al., 2007; Purkait, 2012; Sheng et al., 2010). Educating end users and implementation – and proper application – of precautionary online behaviour are critical in protecting against phishing attacks (Butler, 2007; Purkait, 2012). Although education has its limitations, given the complexity of the problem and a lack of interest by non-specialist Internet users (Jakobsson, 2007), and will not solve the phishing problem on its own (Alsharnouby et al., 2015), aware and vigilant end users who practice precautionary online behaviour are believed to better identify phishing attempts (Purkait et al., 2014).

We focus on one type of behavioural context, that is sharing or disclosing personal information online. We delimit personal information to personally identifying, financial, and demographic information (Norberg et al., 2007). In this study, it explicitly includes: physical address, e-mail address, log-in credentials, bank account number, PIN / one-time security codes, and citizen service number. Thus, we do not include any other information that may be labelled as "personally identifiable information (PII)", such as medical records and biometrics, or other types of private information, such as travel information and family affairs.

Putting personal information (publicly) online provides fraudsters with opportunities to take advantage of that information (Shillair et al., 2015) and to (spear) phish someone. An experimental study in an organizational setting by Rocha Flores et al. (2014) showed that when more target information was added to an attack the likelihood of an organization employee falling for that attack increased. In addition, studies on phishing have demonstrated that an essential part in a fraudulent scheme to be effective is end users give away their personal information, for example user credentials (Hong, 2012; Jansen and Leukfeldt, 2015; Purkait, 2012). Therefore, demonstrating vigilant behaviour towards personal information sharing online is important to (a) prevent being attacked by means of phishing and (b) to prevent phishing attacks from succeeding.

The goal of our study is to gain insight into the effects of fear appeal manipulations on end-users' cognitions and subsequently on danger control (attitude, intentions and behaviour) and on fear control (resistance and avoidance). A novel contribution of this work compared to other research on phishing warnings is a focus on both danger control and fear control, which is ignored in most information security studies that focus solely on danger control (Boss et al., 2015; Wall and Buche, 2017). Additionally, testing the effects of fear appeals in three experimental conditions is not often done in information security studies. Furthermore, most studies within the information security domain focus on behavioural intention only which is considered a drawback (Boss et al., 2015; Crossler et al., 2013). Therefore, we investigate both self-reported behaviour and behavioural intention. Moreover, we examine the effects of fear appeals at two points in time, while most studies examine these at just one point in time (Wall and Buche, 2017). Finally, our study benefits from a large, non-student research sample.

Based on this, our study addresses the following research questions.

Research Question 1: What effect do fear appeals have on end-users' cognitions (perceived vulnerability, perceived severity, fear, response efficacy, self-efficacy and response costs)?

Research Question 2: What effect do fear appeals have on end-users' attitudes towards precautionary online behaviour?

Research Question 3: What effect do fear appeals have on end-users' precautionary online behavioural intentions?

Research Question 4: To what extent is the effect of fear appeals, if any, stable over time?

Research Question 5: What effect do fear appeals have on end-users' self-reported precautionary online behaviour?

2. Theoretical framework

2.1. Protection motivation theory

The leading theoretical framework used for this study is protection motivation theory (Maddux and Rogers, 1983; Rogers, 1975), henceforth PMT, originally developed to study disease prevention and health promotion (Floyd et al., 2000). Although the original purpose of PMT is to clarify fear appeals, it has been used as a more general model to study decisions related to risk (Maddux and Rogers, 1983). Recently, PMT has been applied to the information security domain (e.g., Boehmer et al., 2015; Boss et al., 2015; Jansen and Van Schaik, 2017; Johnston et al., 2015) providing opportunities to study end-users' motivation to perform precautionary online behaviour, a major focus in current (behavioural) information security literature (Boss et al., 2015).

2.2. Threat appraisal

Protection motivation is initiated by two appraisal processes. The

first one is called threat appraisal, a process in which a person evaluates threats triggered by a fear appeal. More specifically, the person evaluates the vulnerability or probability of a threat occurring to him- or herself and the severity or impact of a threat.

PMT studies that examine motivations of end users performing precautionary online behaviour have found mixed results for the threat appraisal process. Some studies found both threat appraisal variables to be significant positive predictors (e.g., Chenoweth et al., 2009; Lee, 2011; Liang and Xue, 2010). However, one study found both threat appraisal variables to be significant, but negative predictors (Crossler, 2010) and in another study perceived vulnerability had a positive influence whereas perceived severity had a negative influence (Ifinedo, 2012). In other cases, only one of two threat appraisal variables were found to be significant predictors (e.g., Gurung et al., 2009; Herath and Rao, 2009; Jansen and Van Schaik, 2017; Vance et al., 2012).

Considering that the above mentioned studies focused on different kinds of protective behaviour within different contexts, it seems that the predictive ability of precautionary behaviour by threat appraisal depends on the threats and behaviours studied (see also Crossler, 2010). Johnston et al. (2015) attributed conflicting outcomes of PMT-variables to the misuse or misspecification of PMT in an information security context, for example by not paying adequate attention to the requirement that fear appeals must be personally relevant to a receiver, or the fact that fear appeals were entirely missing from a study's operationalization.

Personal relevance or issue involvement is deemed essential in communications about information security (Johnston et al., 2015). This factor is especially important since the involvement of the audience in a certain topic determines to what extent one will focus on, elaborate on and comprehend a message (Petty and Cacioppo, 1986), thus potentially influencing the effect of a fear appeal (Johnston et al., 2015). Besides issue involvement, other factors that have an effect on the investment of cognitive resources include time pressure, skill level, and distractions (Luo et al., 2012).

2.3. Coping appraisal

The second appraisal process is called coping appraisal, a process in which a person evaluates components of a fear appeal that relate to possible strategies to prevent threats or to minimize their impact. More specifically, it deals with the person's evaluation of the perceived effectiveness of the recommended response (response efficacy), the perceived ability or skills of oneself to perform the recommended response (self-efficacy) and the perceived barriers in performing the recommended response (response costs), for instance time and expenses (Milne et al., 2000).

Previous work on determinants of precautionary online behaviour shows that response efficacy and self-efficacy are the most influential predictor variables (Boehmer et al., 2015; Crossler, 2010; Ifinedo, 2012; Jansen and Van Schaik, 2017; Lee, 2011; Liang and Xue, 2010). This is also true for studies in the health domain. Indeed, the meta-analyses of Floyd et al. (2000) and Milne et al. (2000) of empirical PMT research and the meta-analysis of Witte and Allen (2000) of empirical research on fear appeals indicated that, in general, the coping variables show stronger relations with adaptive behaviours than the threat variables do.

Response costs have been found to be a significant (negative) predictor of precautionary online behaviour (Chenoweth et al., 2009; Herath and Rao, 2009; Jansen and Van Schaik, 2017; Lee, 2011; Liang and Xue, 2010; Vance et al., 2012) and may play an important part in making security-convenience trade-offs. Herley (2009) argued that end-users make an implicit calculation of costs versus benefits when deciding to follow a certain piece of advice. He claimed, however, that security advice often suffers from a poor trade-off and will therefore be neglected by end users.

2.4. Interventions based on protection motivation theory

When PMT is used as a theoretical basis for interventions, the focus is on the operation of fear appeals, which are “informative communication[s] about a threat to an individual's well-being” (Milne et al., 2000, p. 107). Such communications also contain information on and promote perceptions of efficacy. Therefore, it would seem meaningful to speak of “threat and efficacy appeals”. However, we will use the term “fear appeals” because this is consistent with the literature. Fear appeals thus include elements to raise perceived threat and increase perceived efficacy of a recommended response. The latter seems an important requirement for fear appeals because threat messages in themselves, under low efficacy conditions, have almost no or even negative effects on behaviour (Kok et al., 2014; Peters et al., 2014). Witte and Allen (2000) also stress that fear appeals will only work when complemented by an equally strong efficacy message.

2.5. Protection motivation theory in relation to other theories

Other theories of fear-arousing communications include the parallel process model (Leventhal, 1970), the extended parallel process model (Witte, 1992), henceforth EPPM, and the stage model of processing of fear-arousing communications (Das et al., 2003; De Hoog et al., 2005). A difference between these theories and PMT is that the latter focusses on *danger control* responses only, i.e., an individual performing actions to mitigate a threat. In contrast, the other theories mentioned also focus on *fear control* responses, i.e., actions that do not affect the danger, such as avoidance and emotional coping strategies (De Hoog et al., 2005). In addition, the EPPM also focusses on *non-responses* and the stage model also considers modes and motives of information processing and additional outcome measures, namely attitudes, behavioural intention, and behaviour.

Although PMT is the leading framework in the current study, we apply two additional components of the other theories to provide a more comprehensive view on the effects of the fear appeals studied. The first addition is that we study attitudes – both as an outcome variable and as a predictor of behavioural intention (Fishbein and Ajzen, 2010). This addition is consistent with the EPMM and with previous cybersecurity research using PMT (Jansen and Van Schaik, 2017). The second addition is that we study fear control. According to Witte and Allen (2000), fear appeals often target two types of outcome. Outcomes of the first type are related to message acceptance (danger control), measured in terms of attitude, intentions, and behaviours (i.e., referring to adaptive outcomes). This means that fear needs to be evoked to some degree in order to take appropriate action (Witte et al., 1992). This is also apparent in the “fear of crime” literature, where Hale (1996) argued that people having some degree of concern about crime is a good thing, in order to take action against it. Thus, danger control holds that people use a problem-focused strategy to overcome a certain problem.

However, fear appeals might have a counterproductive effect in terms of outcomes of the second type, message rejection (fear control), such as avoidance, reactance, and denial. This holds that if too much fear is evoked, it will result in a maladaptive outcome (Witte et al., 1992). For example, when a message describes a threat as inevitable and having a high impact, and is not accompanied by an sufficiently easy and effective response to the threat, people might reject the message and use an emotion-focused strategy to change undesirable feelings and emotions towards a problem or threat, without taking actions against the actual threat (Lazarus and Folkman, 1984; Liang and Xue, 2009). Boss et al. (2015) stressed that such possible effects are important to study as well. We adopt two types of message rejection: avoidance or risk denial (i.e., efforts to direct attention away from stress Green et al., 2010) and resistance (i.e., reservations towards the behaviour that is aimed to be changed Van Offenbeek et al., 2013). It could be that the results of acceptance and resistance contradict each other. We adopt the viewpoint of Van Offenbeek et al. (2013) who

conceptualize acceptance and resistance as two separate dimensions rather than an opposite ends of a continuum. In a paper on information system adoption, they showed that on an actor level, ambivalent behaviour does occur, such as “use” and “resistance”. By studying both outcome types, our study provides a unique contribution to behavioural information security research.

2.6. Fear appeal manipulation

A meta-analysis on fear appeals by Witte and Allen (2000) showed that medium to strong effects were achieved by fear manipulations on perceived vulnerability, perceived severity, response efficacy, and self-efficacy. When predictor variables of PMT were manipulated, small significant effects were found for attitudes, behavioural intentions, and behaviours. However, the effects on subsequent behaviour are often limited (Floyd et al., 2000; Milne et al., 2000). For the information security context, studies have demonstrated that fear appeals are effective in promoting precautionary motivations and behaviours (Wall and Buche, 2017).

It is not precisely known which components or types of information in a fear appeal are effective (De Hoog et al., 2005, 2007), although response efficacy and self-efficacy seem more important than raising levels of risk and fear (Ruiter et al., 2014). Also, how fear appeals specifically impact end-user behaviour within the information security context is not yet clear (Johnston et al., 2015; Johnston and Warkentin, 2010). However, a meta-analysis by Sheeran et al. (2014) regarding experimental studies on risk appraisals demonstrated that the largest effect sizes were observed for behavioural intention and behaviour when threat appraisal and coping appraisal variables were simultaneously heightened.

3. Method

3.1. Design

According to Milne et al. (2000) fear appeal intervention studies often comprise between a strong and a weak manipulation. This is because manipulations of argument strength are expected to have an effective impact on message processing (Petty and Cacioppo, 1986).[1] Furthermore, it is argued that argument quality – when processed via the central route – has a positive influence on attitudes (Bhattacherjee and Sanford, 2006; Meijnders et al., 2001). In contrast, Johnston et al. (2015) argue that in information security studies, a strong tradition exists of presenting one (or more than one) treatment to one group and no treatment to a control condition. Our study combined these viewpoints. Therefore we included the following three conditions: a strong intervention (strong fear appeal), a weak intervention (weak fear appeal), and no intervention (control condition). We chose to use an independent-measures design (one group for each condition) because this potentially increases external validity. In addition, it only requires one set of data per participant, making data collection convenient. The possible downside is that individual differences occur between the groups, potentially threatening the internal validity. However, this was limited by using a large sample and a stratified sampling method (controlling for gender and age).

We chose to collect data across two different periods of time. This is because the outcomes of an intervention should be stable over time (Milne et al., 2002). In order to establish this, a decision had to be made about the time between the two measurements. Although an interval can reduce common method biases, when the time frame is too long it can, for example, obscure relationships (Podsakoff et al., 2003). Davinson and Sillence (2010) used a one-week interval for an experimental study on phishing, resulting in positive changes in both intentions and behaviour. Bullée et al. (2016) demonstrated that the effects of an information campaign on social-engineering attacks dissipated already after two weeks. However, a fear-appeal study by Milne et al. (2002), showed that the effects of a PMT-intervention lasted over two weeks. A study on phishing training by Kumaraguru et al. (2009) showed that knowledge retention lasted at least for 28 days. We argue that a timeframe of four weeks is reasonable and also necessary for participants in order to not remember exactly the answers they gave on the first measurement. Furthermore, we believe that a more frequent presentation of a fear appeal message, for example every two weeks, might cause end users information overload. Moreover, by using a four-week period, participants were more likely to encounter situations in which they had to make decisions related to personal information-sharing online. The interval was chosen with the aim of (1) allowing sufficient opportunities for participants to apply the fear appeal messages that were presented and (2) making the second measurement before the effect of the messages have worn off.

At the first measurement (Time 1 [T1]), participants received a strong fear appeal message, a weak fear appeal message or no message, and they all filled out the same questionnaire immediately afterwards. This gave us the opportunity to analyse whether user-perceptions were elevated by means of the (strength of the) fear appeal. We decided not to use a baseline measurement, since it was expected that the study participants already had some beliefs on phishing and on the recommended response. Johnston and Warkentin (2010) noted that fear appeals may reinforce or elevate these beliefs, but in any case users will take action if adequately motivated. The purpose of our study was to investigate the strength of this reaction, justifying our decision to not include a baseline survey. In any case, our control condition provided a baseline comparison with the two experimental groups.

At the second measurement (Time 2 [T2]), participants received a similar questionnaire, including all PMT-related items from the previous questionnaire and their information-sharing behaviour in the past month. This was done to study whether possible effect of the fear appeal would last over time and whether intentions were acted upon.

3.1.1. Fear-appeal design

A meta-analysis of empirical fear appeals research by De Hoog et al. (2007) showed no significant differences between fear appeals that used vivid images and fear appeals that used written information only. Therefore, our study involved the manipulation of a written communication, targeting particular PMT-variables. Following the advice of Kirlappos and Sasse (2012), we focused on equipping “users to assess the potential risks and benefits correctly”, rather than telling them to completely avoid certain kind of behaviour. In addition, we followed their advice in making the fear appeal threat-specific.

The fear appeals were presented by means of a self-developed text, which participants were required to read. The text contained factual information on phishing (victimization) and the effects of sharing personal information online – based on results from Bursztein et al. (2014) and Kloosterman (2015) – and was presented digitally to the participants – within the survey environment. We followed a similar approach like that of De Hoog et al. (2005), by designing a fear appeal with strong arguments and a fear appeal with

[1] The elaboration likelihood model of persuasion (Petty and Cacioppo, 1986) assumes that attitudes are formed by a dual route. When individuals are involved with a certain topic the central route is followed (systematic processing). In that case, individuals actively process a message, because they are motivated and mentally capable of doing so. This might lead to long-term changes in attitudes and, consequently, possibly in behavioural change as well. When individuals lack the aforementioned characteristics, a peripheral route of information-processing is followed, which requires less effort (automated processing). The peripheral route will only lead to temporary attitude change. The content of a message, strong argumentation for example, is not relevant in this case, but the way in which it is presented to an individual, such as attractiveness of the message and reputation of the sender. Thus, the route being followed, or the means in which a message is processed, determines the response.

weak arguments. The PMT-variables perceived vulnerability, perceived severity, response efficacy, and self-efficacy were targeted in the fear appeals because the combined manipulation of threat appraisal and coping appraisal variables showed the largest effect on the outcomes (Sheeran et al., 2014). We also followed a recommendation of Ruiter et al. (2014) by making no emotional statements about threat severity.

Because PMT posits that threat appraisal occurs first (Floyd et al., 2000), the fear appeal messages started by highlighting information regarding phishing vulnerability and severity. We tried to evoke personal relevance by means of perceived vulnerability, addressing the potential of being personally victimized. The emphasis of perceived vulnerability in the strong fear appeal was on the extreme, being almost unable to escape from phishing attacks, whereas the weak fear appeal nuanced the chance of victimization by a phishing attack.

According to PMT, coping appraisal takes place after a threat has been evaluated. Thus, the fear appeal messages continued with information on response efficacy and self-efficacy. Therefore, arguments needed to be constructed that promote the effectiveness and usability of the measure. We primarily focussed on arguments regarding response efficacy, because this variable showed strongest predictive ability in previous research. The emphasis of response efficacy in the strong fear appeal was framed as being very effective, that is not sharing personal information online will lead to not being attacked by phishing and any phishing attack that may happen not being successful. In contrast, in the weak fear appeal the level of efficacy was downgraded.

After the fear appeals were constructed, they were critically reviewed by four of our colleagues who are experts in online safety and security. The expert review led to three main changes: (1) a more active phrasing of sentences, (2) balancing the number of arguments in both fear appeals, and (3) shortening the length of the fear appeals. The fear appeal messages can be found in Appendix A.

3.1.2. Survey questionnaire and procedure

A questionnaire was developed based on a review of the literature, using the following international databases: ACM Digital Library, ScienceDirect and Web of Science. We included items that represent PMT's core predictor variables: perceived vulnerability, perceived severity, response efficacy, self-efficacy, and response costs. The outcome variables were attitude towards behaviour, fear, behavioural intention, online information-sharing behaviour, and message rejection (i.e., resistance and avoidance). Attitude and fear were also identified as predictors of intentions.

The questionnaire items were based on the work of Anderson and Agarwal (2010), Brouwers and Sorrentino (1993), Davis (1993), Ifinedo (2012), Johnston et al. (2015), Milne et al. (2002), Ng et al. (2009), Witte (1994, 1996), and Witte et al. (1998). The items used a 5-point Likert scale (totally disagree – totally agree), with the exception of attitude which used a 5-point semantic differential scale, were translated in Dutch, and were presented in random order. The questionnaire items and the sources we based them on can be found in Appendix B. Before the participants were presented with the items on cognitions, a definition of phishing was given. This was done to ensure that participants would have a common understanding of this threat. The questions regarding behavioural intention and online information-sharing behaviour included a timeframe of four weeks, since time is an important element of behaviour – in addition to action (not sharing or disclosing), target (personal information), and context (online) (Fishbein and Ajzen, 2010). Accordingly, the post-test was conducted four weeks after the pre-test.

The measures related to online information-sharing behaviour were included in both measurements, thus also prior to the intervention (T1), to assess previous information-sharing behaviour (Milne et al., 2002). This was to address a limitation of PMT studies that assume that end users do not already adopt the target coping response (Tanner et al., 1991). Online information-sharing behaviour was measured by means of self-report.[2] The measures on resistance and avoidance were also included in both measurements. We added two additional items for avoidance at T2, because according to Witte (1994), although avoidance occurs immediately, delayed measurements are needed to truly assess avoidance patterns.[3]

It should be noted that, although we rely on previously validated scales, we rely on measuring reactions to the fear appeal by using general measures. Nuanced measures were beyond the scope of the current study and require a qualitative approach diving into the participant's psyche. This means that we rely on analytic truths instead of synthetic truths (Ogden, 2003), which can be considered a limitation and could be addressed in follow-up research.

We also added some supplementary questions, for example, to measure message involvement (Shillair et al., 2015). This was done to check whether respondents had read the fear appeal and whether they consider the information as relevant. In addition, information on demographic characteristics, Internet experience, and phishing awareness were collected. It was sufficient to do this at T1 only because we were able to link the answers of individual participants from both measurements.

Before the data were collected, we conducted a pilot study. First-year bachelor students from NHL Stenden University of Applied Sciences who followed courses in research methods were participants. This was to rectify potential problems before the main study was conducted. The pilot study took place in December 2016 and was conducted on paper. In total, 65 students participated in the pilot of which 33 received the strong manipulation and the other 32 the weak manipulation. All students filled out a supplementary questionnaire with 13 items representing PMT's core variables, 4 items measuring fear, 5 items measuring message rejection, and 12 questions regarding the validity of the fear appeals, i.e., message involvement, argument quality (De Hoog et al., 2005), and also issue derogation and perceived manipulation (Witte et al., 1998). With the exception of message involvement, these constructs were only included in the pilot. All measures used a 5-point Likert scale (1 totally disagree – 5 totally agree); see also Appendix B.

The pilot study resulted in a positive evaluation on the fear appeals. In terms of argument quality the strong and weak fear appeal scored reasonably well, respectively 3.7 and 3.5. The mean scores of issue derogation ($M = 2.3$ in both cases) and perceived manipulation ($M = 2.5$ and $M = 2.2$) can be considered good indicators of the fear appeals not being viewed as overblown or misleading. Reliability scores of the variables were adequate, with the exception of message rejection. We made some adjustments regarding the wording of the items and added an item to improve this. Moreover, instead of measuring message rejection as a single construct, we measured it by means of two constructs in the final questionnaire, namely resistance and avoidance.

An external recruitment service of online panels handled the sampling procedure of participants of the main study. The participants were randomly assigned to one of the experimental conditions (strong fear appeal, weak fear appeal and control condition). By means of stratified random sampling for each condition, we aimed to recruit a representative sample of the Dutch population (by gender and age). We presented the study to the participants as an investigation of Internet users' attitudes and behaviours towards information sharing online and phishing. Anonymity was guaranteed to reduce the likelihood of social desirability in the answers of the participants (Podsakoff et al., 2003). Data collection took place in 2017, between February 28 and March 13 (T1) and the follow-up measurement between April 4 and April 21 (T2). In order to counter possible memory effects, the order of the items was

[2] One could argue that this measure comprises "cognition" instead of "behaviour".

[3] In the further analysis, we use two avoidance constructs: avoidance (measured at T1) and delayed avoidance (measured at T2). See also Appendix C.

changed at T2. As an incentive, the research participants received for their voluntary participation panel points that can be used for discounts at Web shops or for donations to charities.

3.2. Participants

In total, 1219 respondents filled out the questionnaire at T1 and 880 at T2, a retention rate of 72%. We anticipated that fewer participants would partake in the post-test because participation was voluntary. However, measures were taken to enhance the response of the second measurement, for example, by presenting the study as consisting of two parts and by giving participants extra points for their continued participation. The average completion time of the questionnaire for both studies – across the three variants – was 8 min and 21 s (SD = 4 min and 48 s) at T1 and 6 min and 13 s (SD = 3 min and 58 s) at T2.

Eighteen responses at T1 were excluded from data analysis, reducing the set of respondents to 1,201. One was excluded by means of a registration error (recording their age to be 107), ten because of filling out two variants of the questionnaire, two because they had no reference number for comparisons between the datasets, and five because reliability of their answers was in doubt.[4] For T2, the same procedure was carried out, resulting in the exclusion of ten respondents because of filling out two variants of the questionnaire, seventy-four because they had a reference numbers not occurring in T1,[5] one because of a missing reference number and twelve responses due to doubtful reliability. Thus, the net response frequency was reduced to 786, with a net retention rate of 65%. Table 1 presents participant characteristics for each measurement.

We compared our figures (T1) with those of the Dutch population in 2016, as measured by Dutch Statistics' Statline. The gender distribution did not deviate from the Dutch population (χ^2 [1, 1200] = 0.30; p = .863) (Statline, 2017c). Considering age, our sample deviates slightly from the Dutch population (χ^2 [2, 1199] = 6.10; p = .047), with the age group of 40–64 years being somewhat under represented (Statline, 2017c). The age groups that we tested for this comparison were 20–39 (in which we included eleven 19-year olds), 40–64, and 65–80 years. Note that this categorization (from Statline) differs from the one presented in Table 1 (from the response panel). The levels of education differed significantly (χ^2 [2, 1199] = 387.70; p < .001), with the lowest level of education being largely under represented and the highest level of education being largely over represented in our dataset (Statline, 2017b). Regarding work status, participants were more likely to belong to the working population and less likely to the non-working population than the Dutch population (χ^2 [1, 1200] = 54.48; p < .001) (Statline, 2017a). We found no significant differences for demographics between the three measurement groups, in both T1 and T2.

In addition, based on the measurements at T1 (N = 1201), the participants can be considered experienced Internet users, with two-thirds having used it over 15 years (62.9%) and using it for more than 10 h a week (64.0%). Additionally, 70.1% agreed or largely agreed to the statement that they were experienced Internet users. Participants reported to have a rather good understanding of phishing. Three in five (60.1%) claimed to know what phishing is and what can be done to prevent victimization and over a quarter (27.8%) also asserted to know what it entails, but was not sure what can be done against it. One in ten (10.1%) had heard of it, but did not fully understand the details and 2.0% was unaware of its existence. Finally, participants filled out a statement on whether they themselves are primarily responsible for their online safety. Of the participants, 81.2% have agreed or fully agreed with this statement. A neutral opinion was expressed by 11.2% and 7.7% did not (at all) agree.

Table 1
Descriptive statistics.

	Time 1 (N = 1201)		Time 2 (N = 786)	
	Count	Percentage	Count	Percentage
Gender				
Female	608	50.6	382	48.6
Male	593	49.4	404	51.4
Age[a]				
18–34 years	333	27.7	182	23.2
35–49 years	334	27.8	218	27.7
≥50 years	534	44.5	386	49.1
Education				
Low	151	12.6	110	14.0
Medium	421	35.1	263	33.5
High	629	52.4	413	52.5
Work status				
Employed	674	56.1	444	56.5
Not-employed	527	43.9	342	43.5

[a] *Age distribution T1 (M = 47.65,* SD = *16.21); T2 (M = 49.54,* SD = *15.83). The age range was in both measurements 19–76 years.*

3.3. Data analysis

We tested the quality of our data using SmartPLS 2.0 (Ringle et al., 2005).[6] The assessments of reliability and validity can be found in Appendix C. We used SPSS (version 23) for conducting analysis of variance (ANOVA). First, we used one-way between-groups ANOVA to determine the mean differences on the dependent variables across the three different groups (T1). Additional post-hoc tests were used to determine where the differences occurred. Second, we used a mixed-measures ANOVA to determine whether the effect of fear appeals is stable over time (T2 in comparison with T1). These analyses were to answer Research Questions 2–5.

Third, we used the PROCESS macro for SPSS (Hayes, 2016) to conduct multi-categorical mediation analyses (Hayes and Preacher, 2014). Mediation analysis provides information on how effects occur (Hayes, 2014). The idea of mediation in this study is to determine if the effect of the manipulation at T2 runs through the effect at T1. It answers the question whether the effect at T1 is the reason for the effect at T2. If this is not the case (i.e., when a non-significant indirect effect is found), then the effect at T2 cannot be attributed to the effect at T1. We tested this for outcome variables attitude and protection motivation and the predictor variables that were included in the fear appeals: perceived vulnerability, perceived severity, response efficacy, and self-efficacy. This type of analysis provides additional evidence for answering Research Question 5.

Fourth, a Kruskal-Wallis test was used to investigate the difference in self-reported online information-sharing behaviour across the three conditions for T2, providing an answer to Research Question 6.

[4] So-called validator scores (ranging from 0–100) were calculated based on how fast respondents completed the questionnaire, the way grid questions were filled out and how open-ended questions were completed (DataIM, 2008). Scores lower than 50 were closely examined which resulted in leaving participants out when scores were 40 or below. In general, these respondents filled out the questionnaire in just two minutes and/or mostly filled out the neutral option in the grid questions.

[5] These participants were able to participate in T2 due to an error in the invitation process for T2. So-called screen-outs – people that had visited the questionnaire in T1, but could not complete it because the questionnaire had enough participants for certain stratifications – were erroneously also invited for Time 2 (N = 128).

[6] Path models testing PMT predictor variables on fear and protection motivation are the subjects of one of the authors' previous publications (Jansen and Van Schaik, 2018).

4. Results

First, we present the results of the one-way between-groups ANOVA. Second, we highlight the results of the mixed-measures ANOVA. Third, we explore the outcomes of the mediation analysis.

4.1. The effect of fear appeals on outcomes

The participants in the fear appeal conditions were asked about their message involvement – after completing the PMT-items. In the strong-fear appeal condition ($N = 249$), 69.9% (strongly) agreed to the statement of having carefully read the fear appeal message. In the weak fear appeal ($N = 263$), this percentage was 73.0. Respectively 18.1% and 19.0% were neutral and 12.0% and 8.0% (strongly) disagreed with this statement. The second statement regarding message involvement was “the text contains relevant information for me”. In the strong fear appeal, 49.3% (strongly) agreed, 34.9% was neutral and 15.7% (strongly) disagreed with this statement. For the weak fear appeal, these numbers were respectively 50.2%, 33.1% and 16.7%. Considering message involvement, *t*-tests showed no significant differences between both fear appeal conditions.

We conducted a one-way between-groups ANOVA to explore the impact of fear appeals on cognitions, attitude, and online behavioural intentions at T1. Note that the results represent only those respondents who completed both questionnaires ($N = 786$). First, we checked if the assumption of homogeneity was not violated. This was the case, because the Levene's test produced results well above the threshold of 0.05. Although significant effects are visible between the conditions (see Table 2), the actual difference in the mean scores is quite small for all variables. Indeed, the effect sizes, calculated using partial eta squared, were small: $\eta_p^2 = 0.02$ for self-efficacy, 0.01 for perceived vulnerability, response efficacy, attitude, and protection motivation and <0.01 for the remaining variables. Effect sizes are interpreted according to Cohen, (1988) classification scheme (i.e., 0.01 = small; 0.06 = medium; 0.14 = large).

There were significant differences between the conditions on perceived vulnerability, response efficacy, self-efficacy, attitude, and protection motivation. Post-hoc comparisons using the Tukey HSD test indicated that the higher mean scores for the strong fear appeal on perceived vulnerability differed significantly from the weak fear appeal ($p < .05$); the control condition did not differ significantly from either fear appeal conditions. With regard to response efficacy, the higher mean of the strong fear appeal differed significantly from that of the control condition ($p < .05$); the weak fear appeal did not differ significantly from the other two conditions. Considering self-efficacy, the lower mean score of control condition differed significantly ($p < .01$) from that of the strong fear appeal and weak fear appeal; the fear appeal conditions did not differ significantly from each other. A similar pattern was noticeable for attitude and protection motivation. In both instances the mean score of the control condition was significantly lower than the mean scores of the strong fear appeal ($p < .01$) and the weak fear appeal ($p < .05$).

Table 2
Results from one-way between groups ANOVA ($N = 786$).

Constructs	*F (2, 783)*	*p*	η_p^2		Mean, SD
Perceived vulnerability	4.39	.013	0.01	0)	2.54, 0.74
				1)	2.40, 0.76
				2)	2.60, 0.85
Perceived severity	1.73	.178	0.00	0)	3.58, 0.81
				1)	3.68, 0.78
				2)	3.70, 0.77
Fear	0.68	.509	0.00	0)	2.85, 0.94
				1)	2.79, 0.97
				2)	2.88, 0.95
Response efficacy	3.74	.024	0.01	0)	3.70, 0.75
				1)	3.83, 0.71
				2)	3.86, 0.75
Self-efficacy	7.49	.001	0.02	0)	3.26, 0.94
				1)	3.51, 0.84
				2)	3.52, 0.88
Response costs	1.06	.347	0.00	0)	2.98, 0.84
				1)	2.88, 0.83
				2)	2.95, 0.86
Attitude	5.64	.004	0.01	0)	3.60, 0.81
				1)	3.79, 0.80
				2)	3.82, 0.80
Protection motivation	5.96	.003	0.01	0)	3.34, 0.95
				1)	3.57, 0.93
				2)	3.59, 0.94

Note. 0: control condition. 1: weak fear appeal. 2: strong fear appeal.

We conducted a mixed-measures ANOVA to explore whether the effect of fear appeals was stable over time (see Table 3). The main effect of condition was significant for self-efficacy, attitude, and protection motivation and marginally significant for response efficacy. There was a positive small effect of time on most dependent variables and a moderate effect on others (attitude and perceived vulnerability), but not on fear and protection motivation. Only for perceived vulnerability was the main effect of time qualified by a significant interaction effect. This main effect was moderate for weak fear appeal ($d = 0.31$), small for the control condition ($d = 0.20$) and very small for strong fear appeal ($d = 0.09$).

Any differences between the two fear appeal conditions on message rejection variables were small: resistance (T1; strong fear appeal, $M = 2.4$, SD = 0.79; weak fear appeal, $M = 2.4$, SD = 0.80), avoidance (T1; strong fear appeal, $M = 2.6$, SD = 0.91; weak fear appeal, $M = 2.5$, SD = 0.87), and delayed avoidance (T2; strong fear appeal, $M = 2.1$, SD = 0.98; weak fear appeal, $M = 2.2$, SD = 0.94). The *t*-tests showed no significant differences between both fear appeal conditions for these three variables, with effect sizes $d = 0.00$, 0.08, and 0.10, respectively.

4.2. Mediation analysis

We conducted multi-categorical mediation analyses to test the outcome variables attitude and protection motivation (T1) as a mediator of attitude and protection motivation (T2), respectively. Because we have three conditions, dummy variables were created (i.e., D_1 represents the weak fear appeal and D_2 the strong fear appeal, both in comparison with the control condition). Figs. 1–2 present the results of mediation analyses.

In the first two analyses (Figs. 1 and 2), the experimental condition was significant as an indirect positive predictor of attitude/protection motivation (T2), mediated by attitude/protection motivation (T1). However, experimental condition was not significant as a direct predictor of attitude (T2). According to Zhao et al. (2010) classification scheme, these results can be interpreted as indirect-only (full) mediation.

We also conducted mediation analysis for the cognition variables present in the fear appeals (Figs. 3–6). This is important because the mixed-measures ANOVA is only useful to demonstrate any potential interaction effect between time and condition. However, unlike the mediation analysis, this does not address the effect of the manipulation at T2 with the measurement at T1 held constant and as a potential mediator.

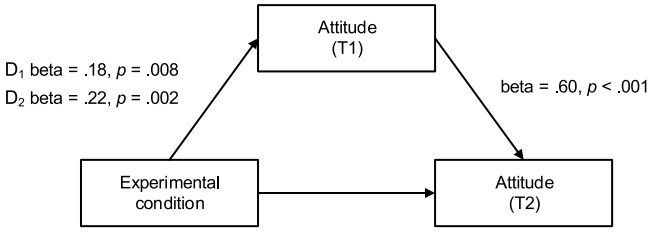
We observe that, similar to attitude and protection motivation, experimental condition was significant as an indirect positive predictor of the coping variables response efficacy and self-efficacy (T2), mediated by respectively response efficacy and self-efficacy (T1), see Figs. 5–6. Furthermore, experimental condition was not significant as a direct predictor in both cases. Thus, these results can be interpreted as indirect-only (full) mediation.

The results from mediation analysis regarding the threat variables perceived vulnerability and perceived severity were less clear, because the lower limits and upper limits included the number of zero in three

Table 3
Results from a mixed-measures ANOVA (N = 786).

Constructs		F (df)	p	η_p^2		M (SD) (T1)	M (SD) (T2)
Perceived vulnerability	C	(2, 783) = 2.00	.136	0.01	0)	2.54 (0.74)	2.68 (0.76)
	T	(1, 784) = 39.95	<.001	0.05	1)	2.40 (0.76)	2.64 (0.79)
	T*C	(2, 783) = 3.70	.025	0.01	2)	2.60 (0.85)	2.68 (0.85)
Perceived severity	C	(2, 783) = 0.77	.462	0.00	0)	3.58 (0.81)	3.70 (0.78)
	T	(1, 784) = 5.12	.024	0.01	1)	3.68 (0.78)	3.70 (0.76)
	T*C	(2, 783) = 1.49	.225	0.00	2)	3.70 (0.77)	3.73 (0.75)
Fear	C	(2, 783) = 0.28	.756	0.00	0)	2.85 (0.94)	2.85 (0.94)
	T	(1, 784) = 1.50	.220	0.00	1)	2.79 (0.97)	2.80 (0.97)
	T*C	(2, 783) = 1.65	.192	0.00	2)	2.88 (0.95)	2.78 (1.01)
Response efficacy	C	(2, 783) = 2.53	.081	0.01	0)	3.70 (0.75)	3.85 (0.75)
	T	(1, 784) = 14.11	<.001	0.02	1)	3.83 (0.71)	3.95 (0.69)
	T*C	(2, 783) = 2.78	.062	0.01	2)	3.86 (0.75)	3.86 (0.78)
Self-efficacy	C	(2, 783) = 5.36	.005	0.01	0)	3.26 (0.94)	3.42 (0.94)
	T	(1, 784) = 7.29	<.01	0.01	1)	3.51 (0.84)	3.59 (0.86)
	T*C	(2, 783) = 2.76	.064	0.01	2)	3.52 (0.88)	3.52 (0.92)
Response costs	C	(2, 783) = 0.99	.373	0.00	0)	2.98 (0.84)	2.86 (0.88)
	T	(1, 784) = 18.45	<.001	0.02	1)	2.88 (0.83)	2.78 (0.80)
	T*C	(2, 783) = 0.13	.880	0.00	2)	2.95 (0.86)	2.82 (0.98)
Attitude	C	(2, 783) = 6.71	.001	0.02	0)	3.60 (0.81)	3.82 (0.89)
	T	(1, 784) = 59.11	<.001	0.07	1)	3.79 (0.80)	4.03 (0.83)
	T*C	(2, 783) = 0.14	.866	0.00	2)	3.82 (0.80)	4.02 (0.88)
Protection motivation	C	(2, 783) = 4.41	.012	0.01	0)	3.34 (0.95)	3.44 (1.03)
	T	(1, 784) = 1.31	.252	0.00	1)	3.57 (0.93)	3.63 (0.98)
	T*C	(2, 783) = 2.39	.092	0.01	2)	3.59 (0.94)	3.53 (1.03)

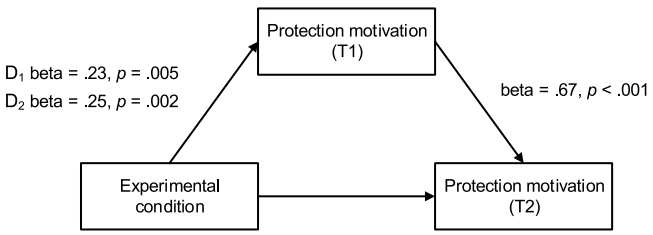
Note. C: condition. T: time. T × C: time × condition. 0: control condition. 1: weak fear appeal. 2: strong fear appeal.



(Relative) direct effects: D_1 beta = .10, p = .128; D_2 beta = .07, p = .265

(Relative) indirect effects: D_1 beta = .11, 95% CI [.03; .20]; D_2 beta = .13, 95% CI [.05; .22]

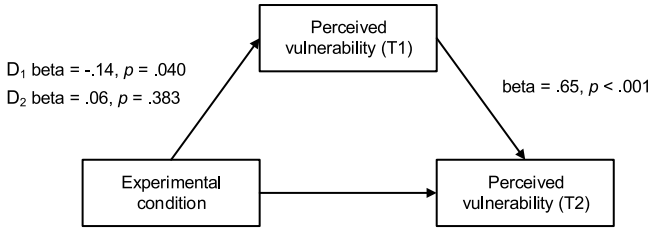
Fig. 1. Model of fear appeal condition as a predictor of attitude (T2) mediated by attitude (T1)



(Relative) direct effects: D_1 beta = .04, p = .576; D_2 beta = -.07, p = .288

(Relative) indirect effects: D_1 beta = .16, 95% CI [.05; .27]; D_2 beta = .17, 95% CI [.06; .29]

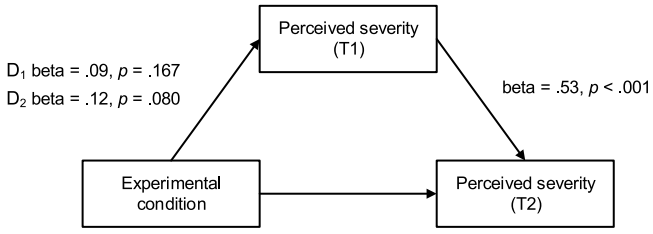
Fig. 2. Model of fear appeal condition as a predictor of protection motivation (T2) mediated by protection motivation (T1).



(Relative) direct effects: D_1 beta = .05, p = .370; D_2 beta = -.04, p = .435

(Relative) indirect effects: D_1 beta = -.09, 95% CI [-.17; -.01]; D_2 beta = .04, 95% CI [-.05; .13]

Fig. 3. Model of fear appeal condition as a predictor of perceived vulnerability (T2) mediated by perceived vulnerability (T1).



(Relative) direct effects: D_1 beta = -.05, p = .353; D_2 beta = -.04, p = .494

(Relative) indirect effects: D_1 beta = .05, 95% CI [-.02; .12]; D_2 beta = .06, 95% CI [-.01; .14]

Fig. 4. Model of fear appeal condition as a predictor of perceived severity (T2) mediated by perceived severity (T1).

of four instances, see Figs. 3–4. This corresponds with a non-significant test result. However, for perceived vulnerability the relative indirect effects of condition (strong fear appeal versus control) was different from zero, which supports the conclusion that M (perceived vulnerability T1) mediates the effect of X (experimental condition) on Y (perceived vulnerability T2) (Hayes and Preacher, 2014).

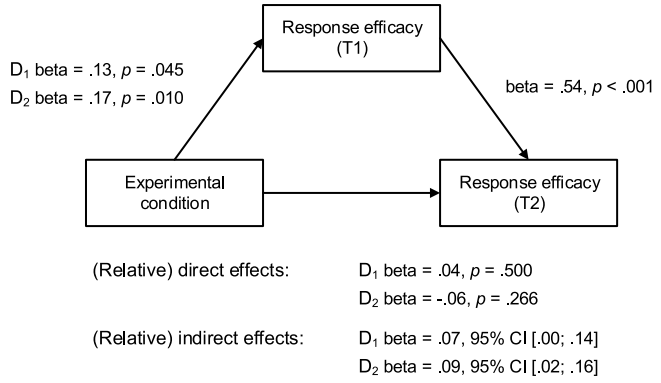


Fig. 5. Model of fear appeal condition as a predictor of response efficacy (T2) mediated by response efficacy (T1).

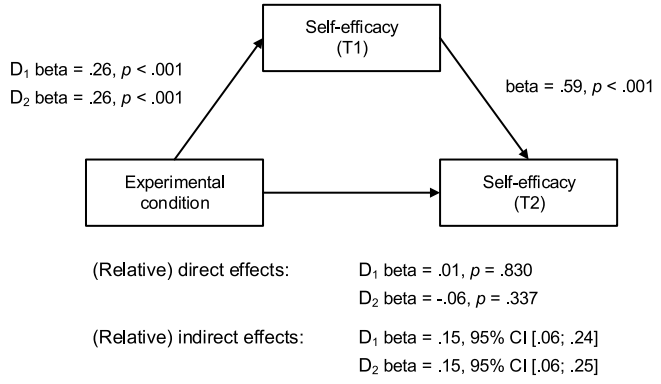


Fig. 6. . Model of fear appeal condition as a predictor of self-efficacy (T2) mediated by self-efficacy (T1).

4.3. Effects on online information-sharing behaviour

Finally, we tested if there was a difference in self-reported online information-sharing behaviour across the three conditions at T2. A Kruskal-Wallis test showed no significant effect of intervention (strong fear appeal, $N = 249$, weak fear appeal, $N = 263$ and control, $N = 274$), χ^2 (2, 786) = 1.14, $\eta_p{}^2 = 0.00$, $p = .567$. Moreover, more than half of all the participants (58.1%) indicated to have shared their personal information both a month prior to T1 and a month prior to T2.

We also tested the level of variance explained for online information-sharing behaviour – using logistic regression. Predictor variables were protection motivation and previous online information-sharing behaviour.[7] The likelihood ratio (R^2_L) is around 0.10 in all three conditions.[8] We find that previous behaviour better predicts behaviour than intentions do in all three conditions. Only in the strong-fear appeal condition was protection motivation a marginally significant predictor of actual behaviour ($p = .085$).

[7] Only self-reported online information-sharing behaviour in the previous month (measured at T1) was used as an additional explanatory variable for self-reported online information-sharing behaviour (measured at T2), because the correlation was well above the threshold of 0.10. Other potential predictor variables, i.e., demographic variables, Internet experience, knowledge on phishing, and level of responsibility did not meet this criterion.

[8] For the strong fear appeal and weak fear appeal conditions, we tested whether the explained variance for behaviour would increase when adding the message rejection variables as additional explanatory variables for self-reported online information-sharing behaviour (measured at T2). This was, however, not the case because it only increased by one hundredth. Only delayed avoidance was a marginally significant predictor of not sharing personal information online (beta = 0.37, $p = .053$).

5. Discussion

We first answer Research Question 1: what effect do fear appeals have on end-users' cognitions? We observed from the one-way between-groups ANOVA that the strong-fear appeal message provided highest mean scores for all predictor variables. The exception was response costs, as predicted, because response costs were not explicitly addressed within the messages, so an effect might not be expected indeed.[9] The scores were, however, only significant for perceived vulnerability in comparison with the weak fear appeal, and for response efficacy and self-efficacy in comparison with the control condition. These results imply that end-users' cognitions can be elevated by means of a fear appeal message, especially when strong arguments are used.

Research Questions 2 and 3 were formulated as follows. What effect do fear appeals have on end-users' (a) attitudes towards precautionary online, and (b) precautionary online behavioural intentions? Again the strong fear appeal produced the highest scores. However, note that the scores were significantly higher only in comparison with the control condition, not the weak fear appeal. This implies that attitudes and behavioural intentions can be raised by making Internet users aware of threats and simultaneously providing behavioural advice on how to mitigate these, which we expected. Protection motivation was heightened, while perceived vulnerability was low, which is a central indicator for personal relevance, and thus an important aspect for how a message is processed. However, according to De Hoog et al. (2007), individuals might still have processed the fear appeal message systematically, because the threat was depicted as severe. They continue by explaining that individuals might find it useful to be well informed, even when the threat is not imminent. This raises the question to what extent the fear appeal elements are salient in all regards which provides interesting leads for future research.

Besides examining protection motivation (danger control), we also looked at three types of fear control (resistance and two avoidance constructs). These constructs were scored low. This is probably due to the low scores on fear as well. Lazarus and Folkman (1984) stress that emotion-focused forms of coping – where fear control can be placed under – tend to be adopted when threat or fear levels are perceived to be high.

We now examine the extent to which the effect of fear appeals was stable over time (Research Question 4). We answer this question first by examining the results from the mixed-measures ANOVA. The results show significant differences in overall mean scores between T1 and T2 for all constructs, except fear and protection motivation. All difference were in the positive direction. Most improvement is found for the constructs perceived vulnerability and attitude. Perhaps, the participants gave the topic at hand (phishing-related security) some thought or spoke about it with others. As a result, they may have realised that one is at risk for falling for phishing scams and sharing personal information online poses avoidable dangers. This positive effect might also be explained by the possibility that filling out a questionnaire such as this one has an awareness-raising effect, since the scores of the control condition were also higher.

The second part of our answer to Research Question 4 is from the results from the mediation analyses. The mediation analyses showed that the fear appeal messages had a significant indirect effect on the second measurement (T2) of outcome variables attitude and protection motivation and PMT variables perceived vulnerability, response efficacy and self-efficacy. This means that the effect of fear appeals at T2 can be attributed to its effect already achieved at T1. For perceived severity no significant indirect effect was observed. Similar to previous studies, the threat-specific variables provide some inconsistencies with what the theory would predict (Wall and Buche, 2017).

Finally, we answer Research Question 5: what effect do fear appeals

[9] Response costs were tested to determine specificity.

have on end-users' precautionary online information-sharing behaviour? The results from the Kruskal-Wallis Test indicate that there was no such effect. The finding that the effects on subsequent behaviour are minor corresponds with results from previous studies (Floyd et al., 2000; Milne et al., 2000). This finding is also in line with previous research in the information security domain which demonstrated that people's positive attitudes towards information security practices do not always correspond with their actual information security behaviour (Spiekermann et al., 2001). Perhaps the fear appeals would have had more effect on behaviour if threat was perceived higher (Boss et al., 2015). Furthermore, we find that previous behaviour better predicts behaviour than intentions do, which is also pointed out by Norman et al. (2005). According to Liang and Xue (2009), people are motivated to repeat previous actions that led to positive outcomes and avoid behaviour that led to negative outcomes.

An alternative explanation is that users might not easily follow up on passive types of advice. A small sample laboratory study performed by Egelman et al. (2008) showed that participants that were prompted by active browser warnings on phishing were more likely to follow the advice given than those who were confronted with passive browser warnings. This is consistent with recent work of Yang et al. (2017) who showed, based on a small sample field experiment, that active phishing warnings seem effective for phishing protection.

Moreover, over half of the participants indicated to have shared their personal information online a month prior to both T1 and T2. In addition, Maloney et al. (2011) propose that if perceived threat is too low to produce fear, end users will take no action instigated by the fear appeal, which might further explain our finding that behaviour did not follow intentions. This is also illustrated by De Hoog et al. (2007, p. 263) who stated "[…], why should anyone invest effort into avoiding a risk, if one does not feel personally at risk?". Follow-up research on fear appeals is needed to find out how behaviour will be impacted when threats do become more personally relevant (i.e., when perceived vulnerability is sufficiently heightened). Additionally, perhaps the perceived benefits of sharing information were perceived higher than the possible risks (Lee et al., 2013).

A possible limitation here, that might have affected the results, is that the behaviour of interest was phrased generally (i.e., not sharing personal information online). Perhaps this behaviour should have been further specified (e.g., not sharing personal information online on unfamiliar locations or to unfamiliar parties or individuals). However, it should be noted that participants reported sharing their information with parties that were both trusted and unfamiliar. Therefore, future research is necessary to find out whether fear appeals would truly modify behaviour. Moreover, we recommend observing actual behaviour in follow-up studies. In addition, stronger results might have been found if one-off behaviour was investigated, such as installing anti-virus software, than repeated behaviours such as in our study (Tannenbaum et al., 2015).

According to our results, end-users' cognitions can potentially be influenced by means of fear appeals. We use the term "potential", because although some of the group differences were significant, the effect sizes were small. An explanation might be that phishing is a well-known threat to Dutch Internet users and it is common knowledge that vigilance is required when sharing personal information online; therefore, the variation was low between the groups. In addition, more variation might have been found if 7-point scales were used. The use of 5-point scales can therefore be seen as a possible limitation of our study.

Because our study took place within participants' social context, we created a realistic setting in which end users read a fear appeal message and answered questions about their cognitions, attitudes and behaviours. This implies, however, that we could not control for the effect of other messages related to safe online practices which were not part of experiment, but which participants may have encountered in their day-to-day use of the Internet, for instance, security notices in e-commerce and social media settings (Benson et al., 2015). Furthermore, we only tested two fear appeal variants, one with strong arguments and one with weak arguments regarding threat and coping appraisal. Future studies could benefit from testing more variants (e.g., strong threat-weak coping, weak threat-strong coping, threat-only and coping-only alternatives). Another issue that needs to be taken into consideration is that we provided the fear appeals within an experimental setting. In real-world situations, these may receive less attention (Wall and Buche, 2017).

To conclude, we acknowledge the fact that other factors can influence the way people process information, for instance communicator factors, such as source credibility and liking of the communicator (O'Keefe, 2016). Briggs et al., (2016) address this point, stating that messenger effects have often been ignored in the cybersecurity domain. Furthermore, other message factors were not addressed, such as personalisation (Davinson and Sillence, 2010), visual elements and humour (Kirlappos and Sasse, 2012). Hence, factors being relevant to a peripheral route of information-processing (Petty and Cacioppo, 1986) were lacking. Future research could focus on such aspects as well, potentially motivating less security-minded Internet users to perform precautionary online behaviour. However, the peripheral route is believed to produce only short-lived effects. This would imply that interventions targeting this route would need to be repeated continuously. In addition, recipient-related individual-difference factors like self-control were not included, which could also have an influence on the outcomes (Michie et al., 2011). However, these factors were outside the scope of the present investigation.

6. Concluding remarks

It is important to note that fear appeals are one of several types of intervention to promote security behaviour against phishing to end users. As noted by Maloney et al. (2011), in the domain of health behaviours, fear appeals might not always be the most appropriate means to do so. Nevertheless, this study demonstrated that fear appeals seem to work for the current context, especially for heightening end-user cognitions, attitudes and behavioural intentions. Fear appeal messages using strong arguments were the most efficacious overall, which is also highlighted by the study of (Boss et al., 2015), but weak arguments still demonstrate efficacy to some extent. Nevertheless, future studies are needed to find out how subsequent behaviour can be improved because results on this crucial aspect seem to lag behind. Qualitative studies focussing on understanding perceptions and reactions to fear appeals might complement the methods presented in this paper. Moreover, follow-up studies are needed to critically evaluate how fear appeals affect end users in the information security domain.

Acknowledgements

This study is part of the Dutch Research Program on Safety and Security of Online Banking. This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy and the Dutch National Police. The funders primarily took on a facilitating role in the entire research process and occasionally provided feedback on written materials, such as the questionnaire and the manuscript.

Appendix A. Fear appeal messages

Strong-fear appeal message (translated from Dutch)

Phishing is increasingly prevalent in the Netherlands and is a common form of online fraud. Research by Statistics Netherlands shows that phishing victimization in the Netherlands occurs in walks of life. Recent scientific research reveals that up to 45% of all people fall for phishing attacks. The chances of getting phished – or already having experienced it – are thus very real.

Phishing attacks are becoming more sophisticated and thus appear more credible. Whereas phishing emails could previously be recognized by spelling mistakes, now-a-days, they look very much like the original mails that are sent by the organization that criminals imitate, are written in proper Dutch and are more personalized. This means that it becomes more difficult to recognize phishing attempts and, therefore, more probable to fall victim to it. When criminals acquire your personal information, they take over your identity with which they perform all kinds of harmful practices such as robbing your bank account and purchasing products on your behalf for which they do not pay.

A phishing attack often starts with receiving a phishing email. A simple and effective way to counter phishing is to be extra careful when handing over your personal information so that you are not at risk of receiving phishing emails. A specific measure that you can take is that you do not share this information online with others, for example, on social media (Facebook, LinkedIn, etc.), on your personal website or when a website asks for it. Research has shown that by taking this simple measure you can prevent a phishing attack on your behalf, or an attack on you will be in vain. Of course, you may need to share such information, for example, when making purchases on a trusted Web shop. The fact remains that you have to deal with your personal information carefully. After all, when you do not meet the recommended measure, you run a very high risk of getting phished.

Weak-fear appeal message

Phishing is a type of online fraud in which people are scammed. Research by Statistics Netherlands shows that 0.4% of the Dutch population has been a victim of phishing in the previous year. Recent scientific research reveals that at least 3% of all people fall for phishing attacks. Therefore, there is a possibility that you will also get phished or that you already have experienced it.

Criminals always find new phishing methods to gain personal information. When criminals acquire such data, they can take over one's identity, for example, to plunder bank accounts or purchase products for which they do not pay. Although the risk of becoming a victim of phishing is small according to research, this can have adverse consequences.

A phishing attack often starts with receiving a phishing email. A simple and effective way to counter phishing is to be extra careful when handing over your personal information so that you are not at risk of receiving phishing emails. A specific measure that you can take is that you do not share this information online with others, for example, on social media (Facebook, LinkedIn, etc.), on your personal website or when a website asks for it. Research has shown that by taking this simple measure you can prevent a phishing attack on your behalf, or an attack on you will be in vain. Of course, you may need to share such information, for example, when making purchases on a trusted Web shop. The fact remains that you have to deal with your personal information carefully. After all, when you do not meet the recommended measure, there is a chance of getting phished.

Appendix B. Questionnaire items

The items of attitude are measured on a semantic differential scale based on the work of Davis (1993) and are operationalized as follows: The online sharing of personal information is: good (1) – bad (5); beneficial (1) – harmful (5); positive (1) – negative (5); wise (1) – foolish (5); favourable (1) – unfavourable (5).

Self-reported information sharing behaviour was measured with the following question: Did you share the following personal information online in the past month? Participants answered this question for the following six types of information: physical address, e-mail address, log-in credentials, bank account number, PIN / one-time security codes, and citizen service number. Self-reported behaviour was measured with a four-point scale: (1) no; (2) once; (3) more than once; (4) do not know. In addition, it was explained that logging into, for example, an e-mail account or an online banking environment was were not considered sharing. For the analysis, the scores on information sharing behaviour were dichotomized and recoded into one variable (yes / no). Prior knowledge of phishing is based on the work of Shillair et al. (2015) and is asked as follows: To what extent are you familiar with phishing? Participants could answer this question in the following ways: I never heard of phishing; I have heard of phishing, but I do not understand the details; I know what phishing is, but I do not know what to do about it; I know what phishing is and how to protect myself against it.

Finally, we based the questions on Internet experience and personal responsibility on previous work of Corbitt et al. (2003) and Boehmer et al. (2015) respectively. Internet experience was asked for by three different questions: a) I have been using the Internet for: less than 1 year; between 1 and 5 years; between 5 and 10 years; between 10 and 15 years; more than 15 years, b) I use the Internet approximately: less than 1 h per week; between 1 and 3 h per week; between 3 and 10 h per week; between 10 and 20 h per week; more than 20 h per week, and c) I perceive myself experienced at using the Internet: 1 strongly disagree – 5 strongly agree. Personal responsibility was also measured on a 5-point Likert scale and was formulated as follows: I am primarily responsible for my safety on the Internet.

Table B1
Instrument (translated from Dutch).

Construct (sources)	Items	
Perceived vulnerability (Witte, 1996)	PV1:	It is likely that I will become victim of phishing
	PV2:	I am at risk for being victimized by phishing
	PV3:	It is possible that I will become victim of phishing
Perceived severity (Johnston et al., 2015; Witte, 1996)	PS1:	If I was a victim of phishing, the consequences would be severe
	PS2:	If I was a victim of phishing, the consequences would be serious
	PS3:	If I was a victim of phishing, the consequences would be significant
Fear (Milne et al., 2002)	FE1:	The thought of becoming a phishing victim makes me feel frightened
	FE2:	The thought of becoming a phishing victim makes me scared
	FE3:	I am anxious about the prospect of becoming a victim of phishing
	FE4:	I am worried about the prospect of becoming a victim of phishing
Response efficacy (Witte, 1996)	RE1:	If I do no share personal information online, then that helps to prevent phishing
	RE2:	I think that not sharing personal information online is an effective means to counter phishing attacks
	RE3:	If I do no share personal information online, then I think the chance decreases of becoming a victim of phishing
Self-efficacy (Witte, 1996)	SE1:	I am able to apply the measure of not sharing personal information online to my Internet behaviour in order to prevent phishing
	SE2:	The measure of not sharing personal information online is easy to use to prevent phishing
	SE3:	Using the recommended measure to not share personal information online to prevent phishing is convenient
Response costs (Ng et al., 2009)	RC1:	Not sharing personal information online is inconvenient
	RC2:	Exercising care when deciding whether or not to share personal information online is time-consuming
	RC3:	Not sharing personal information online requires a lot of mental effort
	RC4:	Not sharing personal information online would require starting a new habit, which is difficult
Protection motivation (Anderson and Agarwal, 2010; Ifinedo, 2012)	PM1:	I am likely to take the measure of not sharing personal information online to protect myself against phishing attacks, for the next month
	PM2:	I would follow the measure of not sharing personal information online to protect myself against phishing attacks, for the next month
	PM3:	I am certain to take the measure of not sharing personal information online to protect myself against phishing attacks, for the next month
	PM4:	It is my intention to take the measure of not sharing personal information online, for the next month
Resistance (Witte et al., 1998; Witte, 1994)	RS1:	Based on what I have read, I do not think it is necessary to protect myself against phishing
	RS2:	After reading the text, I had no inclination to do something against phishing
	RS3:	I think it is unnecessary to protect myself from phishing, even after reading the text
Avoidance (Brouwers and Sorrentino, 1993; Witte et al., 1998)	AV1:	When I read the text, my first instinct was to not want to think about the possibility of being a victim of phishing
	AV2:	If I can avoid thinking of being a victim of phishing, I will do that
	AV3:	I try to avoid thinking about the possibility of becoming a victim of phishing
Delayed avoidance (Witte et al., 1998)	AV4:	In the past month, I have often thought back to the text that I read
	AV5:	I have been thinking a lot about the text I have read over the past month
Message involvement (Shillair et al., 2015)	MI1:	I have read the text carefully
	MI2:	The text contains relevant information for me

Table B2
Pretest items (translated from Dutch).

Construct (sources)	Items	
Argument quality (De Hoog et al., 2005)	AQ1:	Strong arguments are used in the information provided
	AQ2:	The arguments used in the information provided are persuasive
	AQ3:	The information provided contains meaningful arguments
Issue derogation (Witte et al., 1998)	ID1:	The information in the text is exaggerated
	ID2:	The information in the text is overblown
Perceived manipulation (Witte et al., 1998)	MA1:	I feel that the information provided is manipulative
	MA2:	The information provided is misleading

Appendix C. Measurement models

The robustness of the data is tested with reflective and formative measurement models (Hair et al., 2014). Note that the measurement models are tested with T1 data of both experimental conditions ($N = 512$), excluding the data of the control condition ($N = 274$). The rationale for this is that the control condition did not contain data on the resistance and avoidance constructs. Exceptions are the two items representing the delayed avoidance construct (AV4 and AV5), which were measured at T2 only.

Component loadings of the individual items, except three items of the avoidance construct, loaded highly (≥ 0.70) on the corresponding component, providing evidence for uni-dimensionality of the items. However, we had to remove one item of protection motivation (PM3), because this item loaded high on self-efficacy as well (see Table C1).

Instead of using one avoidance construct, we continue with two avoidance constructs, i.e., avoidance and delayed avoidance. We made this distinction guided by (a) the results the full measurement model and (b) because the avoidance construct contained items measured at two different data collection moments (T1 [AV1, AV2, AV3] and T2 [AV4, AV5]), as was suggested by Witte (1994). The item AV2 needed to be removed because it loaded too low on its construct (<0.70). The final measurement model (excluding PM3 and AV2) is presented in Table C2.

Convergent validity was analysed using the average variance extracted (AVE) by a construct from its indicators, which should be 0.7 or higher

Table C1
Full measurement model (N = 512).

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV
PV1	**0.91**	0.15	0.48	−0.10	−0.09	0.38	0.01	0.04	−0.09	0.36
PV2	**0.86**	0.16	0.39	0.00	−0.09	0.32	0.00	0.02	−0.11	0.30
PV3	**0.90**	0.13	0.49	−0.05	−0.13	0.44	0.01	0.01	−0.07	0.42
PS1	0.13	**0.88**	0.31	0.19	0.15	0.04	0.21	0.22	−0.19	0.10
PS2	0.15	**0.93**	0.37	0.20	0.13	0.08	0.22	0.26	−0.20	0.13
PS3	0.16	**0.92**	0.40	0.20	0.11	0.13	0.20	0.21	−0.23	0.12
FE1	0.40	0.37	**0.88**	0.07	0.02	0.32	0.18	0.18	−0.15	0.42
FE2	0.41	0.38	**0.91**	0.07	−0.01	0.38	0.18	0.15	−0.16	0.43
FE3	0.52	0.35	**0.92**	0.02	−0.02	0.36	0.16	0.16	−0.18	0.41
FE4	0.52	0.35	**0.91**	0.04	−0.03	0.37	0.18	0.14	−0.18	0.41
RE1	−0.04	0.15	0.01	**0.74**	0.26	−0.05	0.19	0.22	−0.22	−0.07
RE2	−0.02	0.13	0.08	**0.80**	0.36	−0.06	0.26	0.35	−0.24	0.00
RE3	−0.08	0.23	0.03	**0.86**	0.36	−0.10	0.34	0.34	−0.24	−0.02
SE1	0.05	0.24	0.13	0.48	**0.84**	−0.19	0.42	0.64	−0.30	0.14
SE2	−0.19	0.03	−0.10	0.29	**0.89**	−0.46	0.38	0.59	−0.24	−0.01
SE3	−0.16	0.09	−0.06	0.32	**0.90**	−0.47	0.45	0.69	−0.27	0.01
RC1	0.23	0.03	0.17	−0.15	−0.51	**0.72**	−0.29	0.14	0.14	0.09
RC2	0.35	0.07	0.37	−0.04	−0.22	**0.77**	−0.05	0.05	0.05	0.35
RC3	0.35	0.15	0.37	−0.04	−0.28	**0.81**	−0.03	0.00	0.00	0.29
RC4	0.40	0.05	0.32	−0.07	−0.32	**0.82**	−0.12	0.10	0.10	0.34
AT1	0.00	0.20	0.16	0.33	0.42	−0.11	**0.88**	0.50	−0.30	0.17
AT2	−0.01	0.20	0.14	0.28	0.42	−0.16	**0.86**	0.46	−0.29	0.13
AT3	0.00	0.18	0.18	0.26	0.40	−0.14	**0.90**	0.46	−0.27	0.17
AT4	0.04	0.23	0.20	0.36	0.43	−0.12	**0.88**	0.51	−0.34	0.16
AT5	0.01	0.20	0.18	0.28	0.45	−0.17	**0.92**	0.51	−0.33	0.18
PM1	0.02	0.23	0.17	0.33	0.59	−0.13	0.48	**0.88**	−0.39	0.15
PM2	0.02	0.23	0.17	0.35	0.66	−0.21	0.48	**0.93**	−0.43	0.17
PM3	0.00	0.18	0.13	0.33	0.72	−0.25	0.50	**0.91**	−0.42	0.21
PM4	0.05	0.27	0.16	0.41	0.69	−0.18	0.53	**0.92**	−0.41	0.20
RS1	−0.07	−0.21	−0.17	−0.27	−0.29	0.11	−0.35	−0.38	**0.85**	0.02
RS2	−0.06	−0.13	−0.13	−0.26	−0.27	0.06	−0.29	−0.44	**0.83**	−0.07
RS3	−0.12	−0.23	−0.16	−0.16	−0.18	0.05	−0.17	−0.25	**0.73**	0.11
AV1	0.28	0.02	0.27	−0.06	−0.06	0.35	−0.01	0.00	0.17	**0.63**
AV2	0.20	0.12	0.27	0.08	0.15	0.14	0.18	0.23	−0.04	**0.59**
AV3	0.23	0.03	0.25	−0.07	−0.06	0.27	0.01	0.01	0.18	**0.63**
AV4	0.34	0.12	0.38	−0.03	0.08	0.23	0.21	0.22	−0.11	**0.79**
AV5	0.34	0.14	0.39	−0.02	0.07	0.21	0.22	0.21	−0.11	**0.79**

Note. PV: perceived vulnerability; PS: perceived severity; FE: fear; RE: response efficacy; SE: self-efficacy; RC: response costs; AT: attitude; PM: protection motivation; RS: resistance; AV: avoidance.

Table C2
Final measurement model (N = 512).

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV	AVd
PV1	**0.91**	0.15	0.48	−0.10	−0.09	0.38	0.01	0.04	−0.09	0.24	0.33
PV2	**0.86**	0.16	0.39	0.00	−0.09	0.32	0.00	0.02	−0.11	0.22	0.27
PV3	**0.90**	0.13	0.49	−0.05	−0.12	0.44	0.01	0.02	−0.07	0.31	0.34
PS1	0.13	**0.88**	0.31	0.19	0.15	0.04	0.21	0.23	−0.19	0.00	0.12
PS2	0.15	**0.93**	0.37	0.20	0.13	0.08	0.22	0.27	−0.21	0.03	0.13
PS3	0.16	**0.92**	0.40	0.20	0.11	0.13	0.20	0.22	−0.23	0.04	0.12
FE1	0.40	0.37	**0.88**	0.07	0.02	0.33	0.18	0.19	−0.15	0.30	0.34
FE2	0.41	0.38	**0.91**	0.07	−0.01	0.38	0.18	0.16	−0.16	0.27	0.37
FE3	0.52	0.35	**0.92**	0.02	−0.02	0.36	0.16	0.17	−0.18	0.25	0.37
FE4	0.52	0.35	**0.91**	0.04	−0.03	0.37	0.18	0.14	−0.18	0.27	0.37
RE1	−0.04	0.15	0.01	**0.74**	0.26	−0.05	0.19	0.24	−0.22	−0.11	−0.04
RE2	−0.02	0.13	0.08	**0.80**	0.36	−0.06	0.26	0.35	−0.24	−0.05	0.01
RE3	−0.08	0.23	0.03	**0.85**	0.36	−0.10	0.34	0.34	−0.24	−0.04	−0.04
SE1	0.05	0.24	0.13	0.48	**0.84**	−0.18	0.42	0.63	−0.30	0.02	0.15
SE2	−0.19	0.03	−0.10	0.29	**0.89**	−0.46	0.39	0.56	−0.24	−0.09	0.01
SE3	−0.16	0.09	−0.06	0.32	**0.90**	−0.46	0.45	0.65	−0.27	−0.10	0.04
RC1	0.23	0.03	0.17	−0.14	−0.51	**0.71**	−0.29	−0.32	0.14	0.17	0.04
RC2	0.35	0.07	0.37	−0.04	−0.22	**0.77**	−0.05	−0.05	0.05	0.31	0.25
RC3	0.35	0.15	0.37	−0.04	−0.28	**0.81**	−0.03	−0.07	0.00	0.30	0.19
RC4	0.40	0.05	0.32	−0.07	−0.32	**0.82**	−0.12	−0.14	0.10	0.33	0.24
AT1	0.00	0.20	0.16	0.33	0.42	−0.11	**0.88**	0.48	−0.30	−0.02	0.21
AT2	−0.01	0.20	0.14	0.28	0.42	−0.16	**0.86**	0.46	−0.28	0.00	0.15
AT3	0.00	0.18	0.18	0.26	0.40	−0.13	**0.90**	0.45	−0.27	0.00	0.21
AT4	0.04	0.23	0.20	0.36	0.43	−0.11	**0.88**	0.50	−0.33	0.00	0.19
AT5	0.01	0.20	0.18	0.28	0.45	−0.16	**0.92**	0.50	−0.33	0.00	0.23
PM1	0.02	0.23	0.17	0.33	0.59	−0.12	0.48	**0.90**	−0.39	−0.01	0.18

(*continued on next page*)

Table C2 (*continued*)

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV	AVd
PM2	0.02	0.23	0.17	0.35	0.66	−0.20	0.48	**0.93**	−0.43	−0.01	0.21
PM4	0.05	0.27	0.16	0.41	0.69	−0.18	0.53	**0.93**	−0.41	0.02	0.21
RS1	−0.07	−0.21	−0.17	−0.27	−0.29	0.11	−0.35	−0.37	**0.85**	0.15	−0.07
RS2	−0.06	−0.13	−0.13	−0.26	−0.27	0.06	−0.29	−0.43	**0.83**	0.13	−0.17
RS3	−0.12	−0.23	−0.16	−0.16	−0.18	0.05	−0.17	−0.25	**0.74**	0.21	−0.01
AV1_1	0.28	0.02	0.27	−0.06	−0.06	0.35	−0.01	0.00	0.17	**0.88**	0.24
AV1_3	0.23	0.03	0.25	−0.07	−0.06	0.27	0.01	0.00	0.18	**0.85**	0.24
AV2_4	0.34	0.12	0.38	−0.03	0.08	0.23	0.21	0.21	−0.11	0.26	**0.96**
AV2_5	0.34	0.14	0.39	−0.02	0.07	0.21	0.22	0.20	−0.10	0.27	**0.96**

Note. PV: perceived vulnerability; PS: perceived severity; FE: Fear; RE: response efficacy; SE: self-efficacy; RC: response costs; AT: attitude; PM: protection motivation; RS: resistance; AV: avoidance; AVd: delayed avoidance.

Table C3
Coefficients of discriminant validity ($N = 512$).

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV	AVd
PV	**0.89**										
PS	0.16	**0.91**									
FE	0.51	0.40	**0.91**								
RE	−0.06	0.22	0.05	**0.80**							
SE	−0.12	0.14	−0.01	0.42	**0.87**						
RC	0.43	0.10	0.40	−0.09	−0.42	**0.78**					
AT	0.01	0.23	0.19	0.34	0.48	−0.15	**0.89**				
PM	0.03	0.27	0.18	0.40	0.70	−0.18	0.54	**0.92**			
RS	−0.10	−0.23	−0.19	−0.29	−0.31	0.09	−0.34	−0.44	**0.81**		
AV_1	0.29	0.03	0.30	−0.08	−0.07	0.36	−0.01	0.00	0.20	**0.87**	
AV_2	0.35	0.13	0.40	−0.03	0.08	0.23	0.22	0.22	−0.11	0.28	**0.96**

Note. Off-diagonal values are correlations. Diagonal values are square root of average extracted variances. PV: perceived vulnerability. PS: perceived severity. FE: fear. RE: response efficacy. SE: self-efficacy. RC: response costs. AT: attitude. PM: protection motivation. RS: resistance. AV: avoidance. AVd: delayed avoidance.

(Henseler et al., 2009). Except response efficacy (AVE = 0.64), response costs (AVE = 0.61) and resistance (AVE = 0.65), all values exceeded this cut-off point. Because the AVE values of these three constructs still exceeded 0.50, they were retained in their current form, because more variability in the items of these constructs was accounted for by its component than was not. Construct reliability was assessed using the composite reliability co-efficient. All constructs showed good reliability (≥ 0.84).

Discriminant validity was positively evaluated according the Fornell-Larcker-criterion. This holds that the square root of AVE by each construct from its indicators was greater than its correlation with the remaining constructs (see Table C3). Finally, no multicollinearity issues were observed when testing for this in SPSS; tolerance values were well above 0.10 and VIF values were well below 10.

References

Alsharnouby, M., Alaca, F., Chiasson, S., 2015. Why phishing still works: user strategies for combating phishing attacks. Int. J. Hum. Comput. Stud. 82, 69–82.

Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Q. 34, 613–643.

APWG, 2018. Phishing Activity Trends Report: 1st Quarter 2018. http://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf.

Arachchilage, N.A.G., Love, S., 2014. Security awareness of computer users: a phishing threat avoidance perspective. Comput. Hum. Behav. 38, 304–312.

Arachchilage, N.A.G., Love, S., Beznosov, K., 2016. Phishing threat avoidance behaviour: an empirical investigation. Comput. Hum. Behav. 60, 185–197.

Benson, V., Saridakis, G., Tennakoon, H., Ezingeard, J.N., 2015. The role of security notices and online consumer behaviour: an empirical study of social networking users. Int. J. Hum. Comput. Stud. 80, 36–44.

Bhattacherjee, A., Sanford, C., 2006. Influence processes for information technology acceptance: an elaboration likelihood model. MIS Q. 30, 805–825.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., Cotten, S., 2015. Determinants of online safety behaviour: towards an intervention strategy for college students. Behav. Inf. Technol. 10, 1022–1035.

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 Q. 39, 837–864.

Briggs, P., Jeske, D., Coventry, L., 2016. Behavior change interventions for cybersecurity. In: Little, L., Sillence, E., Joinson, A. (Eds.), Behavior Change Research and Theory: Psychological and Technological Perspectives. Academic Press, pp. 115–135.

Brouwers, M.C., Sorrentino, R.M., 1993. Uncertainty orientation and protection motivation theory: the role of individual differences in health compliance. J. Pers. Soc. Psychol. 65, 102–112.

Bullée, J., Montoya Morales, A., Junger, M., Hartel, P.H., 2016. Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention. In: Proceedings of the Inaugural Singapore Cyber Security R&D Conference, pp. 107–114.

Bursztein, E., Benko, B., Margolis, D., Pietraszek, T., Archer, A., Aquino, A., …, Savage, S., 2014. Handcrafted fraud and extortion: manual account hijacking in the wild. In: Proceedings of the 2014 Conference on Internet Measurement Conference, pp. 347–358.

Butler, R., 2007. A framework of anti-phishing measures aimed at protecting the online consumer's identity. Electron. Lib. 25, 517–533.

Chenoweth, T., Minch, R., Gattiker, T., 2009. Application of protection motivation theory to adoption of protective technologies. In: Proceedings of the 42nd Hawaii International Conference on System Sciences, pp. 1–10.

Cohen, J., 1988. Statistical Power Analysis for the Behavioural Sciences. Lawrence Erlbaum, Mahwah, NJ.

Corbitt, B.J., Thanasankit, T., Yi, H., 2003. Trust and e-commerce: a study of consumer perceptions. Electron. Commerce Res. Appl. 2, 203–215.

Corona, B., Biggio, B., Contini, M., Piras, L., Corda, R., Mereu, M., Mureddu, G., Ariu, D., Roli, F., 2017. DeltaPhish: detecting phishing webpages in compromised websites,. In: Proceedings of European Symposium on Research in Computer Security, pp. 1–16.

Coventry, L., Briggs, P., Jeske, D., Van Moorsel, A., 2014. SCENE: a structured means for creating and evaluating behavioral nudges in a cyber security environment. In: A., Marcus, A. (Eds.), Design, User Experience, and Usability: Theories, Methods, and Tools for Designing the User Experience. Springer, pp. 229–239.

Crossler, R.E., 2010. Protection motivation theory: understanding determinants to backing up personal data. In: Proceedings of the 43rd Hawaii International Conference on System Sciences, pp. 1–10.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101.

Das, E.H., De Wit, J.B., Stroebe, W., 2003. Fear appeals motivate acceptance of action

recommendations: evidence for a positive bias in the processing of persuasive messages. Pers. Soc. Psychol. Bull. 29, 650–664.
DataIM, 2008. Omschrijving Surveyvalidator (Description of the Survey Validator). DataIM, Amsterdam.
Davinson, N., Sillence, E., 2010. It won't happen to me: promoting secure behaviour among internet users. Comput. Hum. Behav. 26, 1739–1747.
Davinson, N., Sillence, E., 2014. Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. Int. J. Hum. Comput. Stud. 72, 154–168.
Davis, F.D., 1993. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. Int. J. Man Mach. Stud. 38, 475–487.
De Hoog, N., Stroebe, W., De Wit, J.B., 2005. The impact of fear appeals on processing and acceptance of action recommendations. Pers. Soc. Psychol. Bull. 31, 24–33.
De Hoog, N., Stroebe, W., De Wit, J.B., 2007. The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: a meta-analysis. Rev. Gen. Psychol. 11, 258–285.
Dhamija, R., Tygar, J.D., Hearst, M., 2006. Why phishing works. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 581–590.
Downs, J.S., Holbrook, M.B., Cranor, L.F., 2006. Decision strategies and susceptibility to phishing. In: Proceedings of the Second Symposium on Usable Privacy and Security, pp. 79–90.
Downs, J.S., Holbrook, M., Cranor, L.F., 2007. Behavioral response to phishing risk. In: Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, pp. 37–44.
Egelman, S., Cranor, L.F., Hong, J., 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1065–1074.
Fishbein, M., Ajzen, I., 2010. Predicting and Changing Behavior: The reasoned Action Approach. Taylor & Francis, New York.
Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. 30, 407–429.
Fransen, M.L., Smit, E.G., Verlegh, P.W., 2015. Strategies and motives for resistance to persuasion: an integrative framework. Front. Psychol. 6, 1–12.
French, J., 2011. Why nudging is not enough. J. Soc. Market. 1, 154–162.
Furnell, S., Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. Comput. Secur. 31, 983–988.
Furnell, S.M., Bryant, P., Phippen, A.D., 2007. Assessing the security perceptions of personal Internet users. Comput. Secur. 26, 410–417.
Green, D.L., Choi, J.J., Kane, M.N., 2010. Coping strategies for victims of crime: effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. J. Hum. Behav. Soc. Environ. 20, 732–743.
Gurung, A., Luo, X., Liao, Q., 2009. Consumer motivations in taking action against spyware: an empirical investigation. Inf. Manag. Comput. Secur. 17, 276–289.
Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2014. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publications, Inc.
Hale C., 1996. Fear of crime: A review of the literature. Int. Review of Victimology, 4, 79–150.
Hayes, A.F., 2014. Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach. Guilford Publications, New York.
Hayes, A.F., 2016. PROCESS (version 2.16). www.processmacro.org.
Hayes, A.F., Preacher, K.J., 2014. Statistical mediation analysis with a multicategorical independent variable. Br. J. Math. Stat. Psychol. 67, 451–470.
Henseler, J., Ringle, C.M., Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing. In: Sinkovics, R.R. (Ed.), Advances in International Marketing Vol. 20. Emerald, Bingley, pp. 277–320.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125.
Herley, C., 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In: Proceedings of the 2009 Workshop on New Security Paradigms Workshop, pp. 133–144.
Hong, J., 2012. The state of phishing attacks. Commun. ACM 55, 74–81.
Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31, 83–95.
Jain, A.K., Gupta, B.B., 2017. Two-level authentication approach to protect from phishing attacks in real time. J. Ambient Intell. Hum. Comput. 1–14. https://doi.org/10.1007/s12652-017-0616-z.
Jakobsson, M., 2007. The human factor in phishing. Privacy Secur. Consum. Inf. 7, 1–19.
Jansen, J., Leukfeldt, R., 2015. How people help fraudsters steal their money: an analysis of 600 online banking fraud cases. In: Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust, pp. 24–31.
Jansen, J., Van Schaik, P., 2017. Comparing three models to explain precautionary online behavioural intentions. Inf. Comput. Secur. 25, 165–180.
Jansen J., Van Schaik P., 2018. Persuading end users to act cautiously online: A fear appeals study on phishing, *Inf. & Comput. Secur.* 26, 264–276.
Joel, D., Jain, A.K., 2018. Mobile phishing attacks and defence mechanisms: state of art and open research challenges. Comput. Secur. 73, 519–544.
Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34, 549–566.
Johnston, A.C., Warkentin, M., Siponen, M.T., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. 39, 113–134.
Kahneman, D., 2011. Thinking, Fast and Slow. Penguin Group, London, UK.
Kirlappos, I., Sasse, M.A., 2012. Security education against phishing: a modest proposal for a major rethink. IEEE Secur. Privacy 24–32 2012.
Kloosterman, R., 2015. Slachtofferschap Cybercrime En Internetgebruik [Cybercrime Victimization and Internet Use]. Statistics Netherlands, The Hague.
Kok, G., Bartholomew, L.K., Parcel, G.S., Gottlieb, N.H., Fernández, M.E., 2014. Finding theory- and evidence-based alternatives to fear appeals: intervention mapping. Int. J. Psychol. 49, 98–107.
Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., Pham, T., 2009. School of phish: a real-world evaluation of anti-phishing training. In: Proceedings of the 5th Symposium on Usable Privacy and Security, pp. 1–12.
Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Sci. 3, 1–10.
Lazarus, R.S., Folkman, S., 1984. Stress, Appraisal, and Coping. Springer Publishing Company, New York.
Lee, Y., 2011. Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective. Decis. Support Syst. 50, 361–369.
Lee, H., Park, H., Kim, J., 2013. Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. Int. J. Hum. Comput. Stud. 71, 862–877.
Leventhal, H., 1970. Findings and theory in the study of fear communications. Adv. Exp. Soc. Psychol. 5, 119–186.
Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS Q. 33, 71–90.
Liang, H., Xue, Y., 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. 11, 394–413.
Ludl, C., McAllister, S., Kirda, E., Kruegel, C., 2007. On the effectiveness of techniques to detect phishing sites. In: Proceedings of the Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 20–39.
Luo, X.R., Zhang, W., Burd, S., Seazzu, A., 2012. Investigating phishing victimization with the heuristic-systematic model: a theoretical framework and an exploration. Comput. Secur. 38, 28–38.
Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19, 469–479.
Maloney, E.K., Lapinski, M.K., Witte, K., 2011. Fear appeals and persuasion: a review and update of the extended parallel process model. Soc. Pers. Psychol. Compass 5, 206–219.
Meijnders, A.L., Midden, C.J., Wilke, H.A., 2001. Communications about environmental risks and risk-reducing behavior: the impact of fear on information processing. J. Appl. Soc. Psychol. 31, 754–777.
Michie, S., van Stralen, M.M., West, R., 2011. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implementation Sci. 6, 1–11.
Milne, S., Orbell, S., Sheeran, P., 2002. Combining motivational and volitional interventions to promote exercise participation: protection motivation theory and implementation intentions. Br. J. Health Psychol. 7, 163–184.
Milne, S., Sheeran, P., Orbell, S., 2000. Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. J. Appl. Soc. Psychol. 30, 106–143.
Ng, B.-Y., Kankanhalli, A., Xu, Y.C., 2009. Studying users' computer security behavior: a health belief perspective. Decis. Support Syst. 46, 815–825.
Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. J. Consum. Affairs 41, 100–126.
Norman, P., Boer, H., Seydel, E.R., 2005. Protection motivation theory. In: Conner, M., Norman, P. (Eds.), Predicting Health Behaviour. Open University Press, pp. 81–126.
Ogden, J., 2003. Some problems with social cognition models: A pragmatic and conceptual analysis. Health Psychol. 22, 424–428.
O'Keefe, D.J., 2016. Persuasion: Theory and Research (third edition). SAGE Publications.
Peters, G.-J.Y., Ruiter, R.A., Kok, G., 2014. Threatening communication: a qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals. Int. J. Psychol. 49, 71–79.
Petty, R.E., Cacioppo, J.T., 1986. The elaboration likelihood model of persuasion. In: Berkowitz, L. (Ed.), Advances in Experimental Social Psychology 19. Academic Press, New York, pp. 123–205.
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. J. Appl. Psychol. 88, 879–903.
Posey, C., Roberts, T.L., Lowry, P.B., 2015. The impact of organizational commitment on insiders' notivation to protect organizational information assets. J. Manag. Inf. Syst. 32, 179–214.
Purkait, S., 2012. Phishing counter measures and their effectiveness - literature review. Inf. Manag. Comput. Secur. 20, 382–420.
Purkait, S., Kumar De, S., Suar, D., 2014. An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. Inf. Manag. Comput. Secur. 22, 194–234.
Ringle, C.M., Wende, S., Will, A., 2005. SmartPLS 2.0.M3. SmartPLS, Hamburg Retrieved from. http://www.smartpls.com.
Rocha Flores, W., Holm, H., Svensson, G., Ericsson, G., 2014. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Inf. Manag. Comput. Secur. 22, 393–406.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91, 93–114.
Ruiter, R.A.C., Kessels, L.T.E., Peters, G.-J.Y., Kok, G., 2014. Sixty years of fear appeal research: current state of the evidence. Int. J. Psychol. 49, 63–70.
Sasse, M.A., Brostoff, S., Weirich, D., 2001. Transforming the "weakest link" — a human/computer interaction approach to usable and effective security. BT Technol. J. 19, 122–131.
Sheeran, P., Harris, P.R., Epton, T., 2014. Does heightening risk appraisals change people's intentions and behavior? A meta-analysis of experimental studies. Psychol. Bull.

140, 511–543.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J., 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 373–382.
Shillair, R., Cotten, S.R., Tsai, H.-Y.S., Alhabash, S., LaRose, R., Rifon, N.J., 2015. Online safety begins with you and me: convincing Internet users to protect themselves. Comput. Hum. Behav. 48, 199–207.
Spiekermann, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce, pp. 38–47.
Statline, 2017. Arbeidsdeelname: Kerncijfers (Rate of employement: Key figures). http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLnl&PA=82309NED&LA=nl.
Statline, 2017. Bevolking: hoogst behaald onderwijsniveau; geslacht, leeftijd en herkomst (Population: hightest attained level of education; gender, age and origin). http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLnl&PA=82275NED&LA=nl.
Statline, 2017. Bevolking: Kerncijfers (Population: Key figures). http://statline.cbs.nl/StatWeb/publication/?PA=37296ned&D1=a&D2=0,10,20,30,40,50,60,(l-1),l&HDR=G1&STB=T.
Tannenbaum, M.B., Hepler, J., Zimmerman, R.S., Saul, L., Jacobs, S., Wilson, K., Albarracín, D., 2015. Appealing to fear: a meta-analysis of fear appeal effectiveness and theories. Psychol. Bull. 141, 1178–1204.
Tanner, J.F., Hunt, J.B., Eppright, D.R., 1991. The protection motivation model: a normative model of fear appeals. J. Market. 55, 36–45.
Thaler, R.H., Sunstein, C.R., 2009. Nudge: Improving Decisions About Health, Wealth and Happiness. Penguin Group, London, UK.
Van Offenbeek, M., Boonstra, A., Seo, D., 2013. Towards integrating acceptance and resistance research: evidence from a telecare case study. Eur. J. Inf. Syst. 22, 434–454.
Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P., 2017. Risk perceptions of cyber-security and precautionary behaviour. Comput. Hum. Behav. 75, 547–559.
Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. 49, 190–198.
Wall, J.D., Buche, M.W., 2017. To fear or not to fear? A critical review and analysis of fear appeals in the information security context. Commun. Assoc. Inf. Syst. 41, 277–300.
Witte, K., 1992. Putting the fear back into fear appeals: the extended parallel process model. Commun. Monographs 59, 329–349.
Witte, K., 1994. Fear control and danger control: a test of the extended parallel process model (EPPM). Commun. Monographs 61, 113–134.
Witte, K., 1996. Predicting risk behaviors: development and validation of a diagnostic scale. J. Health Commun. 1, 317–341.
Witte, K., Allen, M., 2000. A meta-analysis of fear appeals: implications for effective public health campaigns. Health Educ. Behav. 27, 591–615.
Witte, K., Berkowitz, J.M., Cameron, K.A., McKeon, J.K., 1998. Preventing the spread of genital warts: using fear appeals to promote self-protective behaviors. Health Educ. Behav. 25, 571–585.
Yang, W., Xiong, A., A., Chen, J., Proctor, R.W., Li, N, 2017. Use of phishing training to improve security warning compliance: evidence from a field experiment. In: Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp, pp. 52–61.
Zhao, X., Lynch, J.G., Chen, Q., 2010. Reconsidering Baron and Kenny: myths and truths about mediation analysis. J. Consum. Res. 37, 197–206.