Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Persuading End Users to Act Cautiously Online: Initial Findings of a Fear Appeals Study on Phishing

J. Jansen[1,2] and P. van Schaik[3]

[1]Faculty of Humanities and Law, Open University of the Netherlands
[2]Cybersafety Research Group, NHL University of Applied Sciences
[3]School of Social Sciences, Business and Law, Teesside University
e-mail: j.jansen@nhl.nl; p.van-schaik@tees.ac.uk

Abstract

This study examined the impact of fear appeals on user cognitions and behavioural intentions with regard to minimizing the threat of phishing attacks. 1,201 Internet users filled out an online survey and were presented with one of three fear appeal conditions: strong fear appeal, weak fear appeal and no fear appeal. Arguments regarding perceived vulnerability of phishing attacks and arguments concerning response efficacy of vigilant online information-sharing behaviour were manipulated in the fear appeals. Analysis of variance showed that the strong fear appeal message elevated threat appraisal, coping appraisal and protection motivation. Partial least squares path modelling showed little variation between the three groups concerning explained variance of protection motivation and fear. Nonetheless, we conclude that precautionary online behavioural intentions can be raised by making Internet users aware of the threat while simultaneously providing behavioural advice on how to mitigate this threat.

Keywords

Information Security Behaviour, Fear Appeals, Protection Motivation Theory, Phishing, Online Information-sharing Behaviour, Human Factors

1. Introduction

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). Nonetheless, people play an important role in protecting themselves against such incidents, because they form a crucial link in the information security chain.

The current study focusses on the protection against a specific online threat, namely phishing, i.e., the process of retrieving personal information using deception through impersonation (Lastdrager, 2014). Phishing is considered predominantly dangerous to Internet users (Arachchilage *et al.* 2016) and forms a world-wide problem (APWG, 2015) for different sectors, such as retail and banking.

Security education, training and awareness, and the implementation – and proper application – of precautionary online behaviour are critical in protecting against

phishing attacks (Purkait, 2012). Although these efforts will not solve the phishing problem on its own (Alsharnouby *et al.* 2015), aware and vigilant Internet users who practice precautionary online behaviour are believed to better identify phishing attempts (Purkait, 2012). However, transforming the Internet population into an aware and vigilant audience is not easy, as it is not precisely known which interventions work best.

This study contributes to improving online security by investigating to what extent fear appeals can persuade Internet users to perform safe online behaviour and using protection motivation theory (Maddux and Rogers, 1983; Rogers, 1975) as its theoretical basis. Fear appeals are 'informative communication[s] about a threat to an individual's well-being' (Milne *et al.* 2000, p. 107) that also contain information on promoting perceptions of efficacy. Attention to fear and fear appeals is currently lacking in the information security domain (Johnston *et al.* 2015).

We focus on one type of behavioural context: sharing or disclosing personal information online. Personal information includes personally identifying, financial and demographic information (Norberg *et al.* 2007). When people put their personal information online, it makes it easy for perpetrators to, for example, (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 employee falling for that attack increased. In addition, studies on phishing have demonstrated for a fraudulent scheme to be effective it is essential that people give away their personal information, for example, user credentials (e.g., Jansen and Leukfeldt, 2015). Thus, 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.

This paper highlights the preliminary results of a pre-test-post-test design using fear appeal manipulations. The results from the pre-test are central to this paper. The main goal is to gain insight into the effects of fear appeal manipulations on Internet users' cognitions and subsequently on protection motivation, i.e., message acceptance. In sum, our study will answer the following two research questions.

1) What effect do fear appeals have on Internet users' cognitions (perceived vulnerability, perceived severity, fear, response efficacy, self-efficacy, response costs)?

2) What effect do fear appeals have on precautionary online behavioural intentions of Internet users?

The results of the post-test will also include measures of attitude, subsequent (self-reported) behaviour and two types of message non-acceptance, i.e., resistance and avoidance. These variables are adopted from the extended parallel process model (Witte, 1992) and the stage model of processing of fear-arousing communications (De Hoog *et al.* 2005), which are other theories of fear-arousing communications.

2. Background

The purpose of protection motivation theory (henceforth PMT) is to clarify fear appeals, but it has also been used as a more general model to study decisions related to risk (Maddux and Rogers, 1983). PMT has been recently used in the information security domain and is considered to be a useful theory for predicting different types of precautionary behaviour (e.g., Jansen and Van Schaik, 2017).

PMT posits that intentions to perform precautionary behaviour, i.e., protection motivation, are initiated by the threat appraisal process: an evaluation of the perceived vulnerability and severity of a possible threat that is triggered by a fear appeal. This is followed by the coping appraisal process, in which a particular response to mitigate or minimize the threat is evaluated, based on the perceived efficacy of this response, the perceived self-efficacy of executing or adopting the response and the costs that are associated with performing the coping response.

Prior research shows that response efficacy and self-efficacy are the most influential predictors for precautionary online behaviour (e.g., Boehmer *et al.* 2015; Jansen and Van Schaik, 2017), which is also true for studies in the health domain. Hence, the meta-analyses of Floyd *et al.* (2000) and Milne *et al.* (2000) on PMT and the meta-analysis of Witte and Allen (2000) on fear appeals indicate that the coping variables generally show stronger relations with adaptive behaviours than the threat variables do. However, besides increasing the perceived efficacy of a recommended response, raising perceived threat in a fear appeal is still important because threat appraisal initiates coping appraisal. Finally, Witte and Allen (2000) stress that fear appeals will only work when complemented by an equally strong efficacy message.

3. Method

In this section, we describe the methods used to answer the research questions. First, we discuss the survey questionnaire, procedure and participants. Second, we discuss the design of the fear appeals. Third, we discuss data analysis, validity and reliability of measures. Detailed information about the methods and measures are available from the authors upon request.

3.1. Survey questionnaire, procedure and participants

A survey design was used to experimentally manipulate fear appeals. Sampling was done by an external recruitment service of online survey panels. Participants received panel points that can be used for discounts at web shops and for donations to charities as compensation for their voluntary participation. The participants were randomly assigned to one of three experimental groups. Stratified sampling was applied for group composition – controlling for gender and age – resulting in equivalent groups as demonstrated by the results form subsequent analysis of variance (ANOVA).

The survey started by asking participants their demographic characteristics, making it possible to control whether the quotas of certain strata were reached. Thereafter, participants answered questions regarding their Internet experience and online behaviour concerning sharing personal information. This was followed by the fear appeal manipulation – a written text within the survey environment. One group read a strong fear appeal message with strong arguments, one group read a weak fear appeal message with weak arguments and a control group received no message. Immediately after the message, participants filled out questions – on a 5-point Likert scale (1 totally disagree – 5 totally agree) – representing PMT's core variables.

The study was conducted with 1,219 Dutch Internet users, between February 28 and March 13, 2017. After excluding 18 participants, the net response was 1,201 of whom 400 were in the strong-fear appeal group, 397 in the weak-fear appeal group and 404 in the control group. In total, 50.6% women and 49.4% men participated. The mean age of participants was 47.7 years (SD = 16.2) and the age range was 19-76 years. Their levels of education were 12.6% low, 35.1% medium and 52.4% high.

3.2. Fear appeal design

Like most PMT studies, our study involved manipulating a written communication, targeting PMT-variables. Both the strong and weak fear appeal message included factual information on the vulnerability and severity of phishing attacks, appealing to threat appraisal. The combination of manipulated threat appraisal and coping appraisal variables showed the largest effect on outcomes in earlier studies (Sheeran *et al.* 2014). Therefore, our messages also contained information on how to mitigate phishing attacks by means of being vigilant when sharing personal information online (the suggested coping response). For coping appraisal, specific information was included appealing to response efficacy and self-efficacy.

In the strong fear appeal message, strong arguments were presented regarding perceived vulnerability (being almost unable to escape from phishing attacks), whereas the weak fear appeal message used weak arguments nuancing the chances to be victimized by a phishing attack. For coping appraisal, the primary focus was on arguments regarding response efficacy, because this variable showed strongest predictive ability in previous research. The strong fear appeal used strong arguments framing the response 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, the weak fear appeal used weak arguments downgrading the level of efficacy.

The fear appeals were critically reviewed by four of our colleagues for refinement purposes, who are experts in the field of online safety and security. The fear appeals and their arguments were also piloted using 65 first-year bachelor students from NHL University of Applied Sciences who followed courses in research methods. The pilot study resulted in a positive evaluation of the fear appeals, with specific items measured on a 5-point Likert scale (1 totally disagree – 5 totally agree). In terms of argument quality (De Hoog *et al.* 2005), the strong fear appeal (N = 33) and weak

fear appeal (N = 32) 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 messages not being viewed as exaggerated and manipulative (Witte *et al.* 1998).

3.3. Data-analysis, validity and reliability

Validated scales were adopted from previous studies and mostly used 3 items, except for fear, response costs and protection motivation, which used 4. The items were translated in Dutch and were presented in random order. Two examples of items are: a) the thought of becoming a phishing victim makes me feel frightened (FE1) and b) I am likely to take the measure of not sharing personal information online to protect myself against phishing in the coming month (PM1). A timeframe of one month was included here, because the post-test took place four weeks after the pre-test.

One-way between-groups ANOVA was used to determine the mean differences on the dependent variables between the three different groups. Additional post-hoc tests were used to determine where the differences occurred. The analyses were conducted with SPSS (Version 23).

Partial least squares path modelling (henceforth PLS), using SmartPLS 2.0 (Ringle *et al.* 2005), was used to emphasize differences in model results between the three conditions. Analysis of cross loadings from the measurement model indicated that one item for protection motivation (PM3) had to be excluded. PM3 loaded too high on self-efficacy (≥ .70). Construct reliability, analysed using the composite reliability coefficient, was good (≥ .85 for all constructs). Analysis of convergent validity, using the average variance extracted (AVE), led to the exclusion of one additional item for response costs (RC2). With the exception of response efficacy (.66) and response costs (.66), all constructs met the AVE cut-off point of .70. However, more variability of the response efficacy and response costs constructs was accounted for than not (> .50). According to the Fornell-Larcker criterion, discriminant validity was in order, meaning that the square root of AVE for each construct was greater than its correlation with the remaining constructs. Additional SPSS analysis showed tolerance values well above .10 and VIF values well below 10, indicating no multi-collinearity issues. We used a standard bootstrapping procedure (N = 5,000) to test the significance of the structural models' parameters (Henseler *et al.* 2009).

4. Results

A one-way between-groups ANOVA was conducted to explore the impact of fear appeals on cognitions and protection motivation. Although most cognitions showed a significant effect between the groups (see Table 1; 1 = strong-fear appeal group, 2 = weak-fear appeal group, 3 = control group), the actual difference in the mean scores between the groups was quite small for all variables. Indeed, the effect sizes, calculated using eta squared, were small (.01 for the treat appraisal and fear variables, 0.2 for self-efficacy and < .01 for response efficacy and response costs).

Effect sizes are interpreted according to Cohen's (1988) classification scheme (i.e., .01 = small, .06 = medium, .14 = large).

Constructs	***(df) F***	***p***	**Means and standard deviations**
Perceived vulnerability	(2, 1198) = 4.19	$p = .015$	1) M = 2.56, SD = .82 2) M = 2.41, SD = .77 3) M = 2.53, SD = .73
Perceived severity	(2, 1198) = 3.68	$p = .026$	1) M = 3.68, SD = .79 2) M = 3.66, SD = .78 3) M = 3.54, SD = .82
Fear	(2, 1198) = 3.31	$p = .037$	1) M = 2.92, SD = .95 2) M = 2.74, SD = .97 3) M = 2.82, SD = .96
Response efficacy	(2, 1198) = 2.64	$p = .072$	1) M = 3.82, SD = .78 2) M = 3.81, SD = .72 3) M = 3.71, SD = .76
Self-efficacy	(2, 1198) = 9.56	$p < .001$	1) M = 3.53, SD = .87 2) M = 3.49, SD = .86 3) M = 3.28, SD = .92
Response costs	(2, 1198) = 2.94	$p = .053$	1) M = 2.98, SD = .91 2) M = 2.87, SD = .86 3) M = 3.01, SD = .88

Table 1: Results from one-way between groups ANOVA (N = 1,201)

Considering perceived vulnerability and fear, post-hoc comparisons using the Tukey HSD test indicated that the higher mean scores for the strong-fear appeal group differed significantly from the weak-fear appeal group ($p < .05$); the control group did not differ significantly from either fear appeal group. With regard to perceived severity, the higher mean of the strong-fear appeal group differed significantly from that of the control group ($p < .05$); the weak-fear appeal group did not differ significantly from the other two groups. Considering self-efficacy, the lower mean score of the control group differed significantly from that of the strong-fear appeal group ($p < .001$) and weak-fear appeal group ($p < .01$); the fear appeal groups did not differ significantly from each other.

Protection motivation was tested next. There was a statistically significant difference in the mean scores for protection motivation across the three groups F (2, 1198) = 11.27, $p < .001$. The effect size was .02. Post-hoc comparisons indicated that the lower mean score for the control group (M = 3.31, SD = .96) was significantly different from the strong-fear appeal group (M = 3.60, SD = .93) and the weak-fear appeal group (M = 3.57, SD = .91), both at a significance level of $p < .001$. Both fear appeal groups did not differ significantly from each other.

The structural models of the three conditions – using PLS – are presented in Figures 1-3. A substantial amount of variance in protection motivation was explained in all

three conditions ($R^2 \approx 55\%$). The amount of variance explained in fear was lower, but quite similar in all three conditions ($R^2 \approx 35\%$).

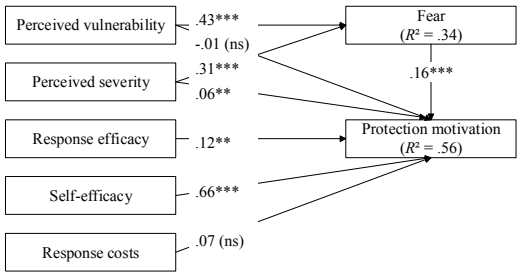

Figure 1: Structural model, strong-fear appeal group (N = 400)

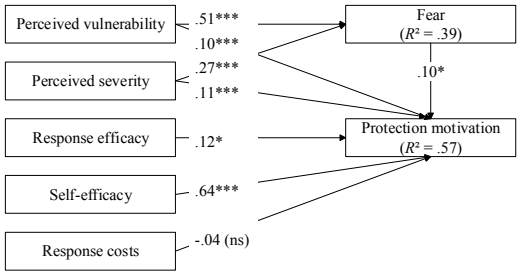

Figure 2: Structural model, weak-fear appeal group (N = 397)

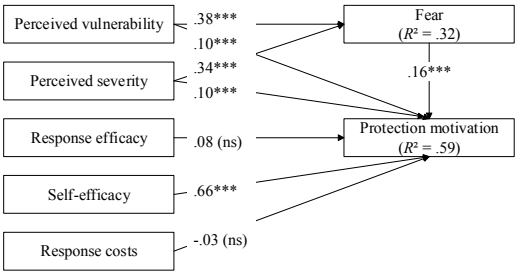

Figure 3: Structural model, control group (N = 404)

First, the results show that response cost was not a significant predictor of protection motivation in any of the three conditions. Second, perceived severity, fear, response efficacy and self-efficacy remained significant predictors of protection motivation under the strong fear appeal, but the predictive power of perceived vulnerability on protection motivation disappeared. Under the weak fear appeal, all predictors from PMT, except for response costs, were significant and in the proposed direction. Furthermore, considering the manipulated variables in the fear appeal messages, response efficacy was not a significant predictor of protection motivation in the control group, while perceived vulnerability was.

5. Discussion and Conclusion

We observed from the ANOVA analyses that the strong fear appeal message provided highest scores for the two threat appraisal variables and for fear. This is also true for the coping variables, with the exception of response costs. Response costs were, however, not explicitly addressed within the fear appeals, so an effect might not be expected. Protection motivation was highest for the two groups who received a fear appeal message. This means that behavioural intentions can be raised by a combination of making Internet users aware of threats and providing behavioural advice on how to mitigate these, regardless of argument strength. The extent to which behaviour follows intention will be tested in future work.

From the PLS analyses, we observed that response cost was not a significant predictor of protection motivation. Thus, it seems that the participants are not bothered by the perceived costs of the presented coping measure. We also found that in the strong fear appeal condition, perceived vulnerability was no direct predictor of protection motivation, as opposed to the other conditions. Perhaps increased fear cancels out the direct influence of this variable on protection motivation. A possible reason for response efficacy not being a predictor and perceived vulnerability being a predictor of protection motivation in the control group is that vulnerability to phishing is easier to imagine than the efficacy of not sharing personal information online. Follow-up research is required to test these conjectures.

According to our results, Internet users' cognitions can potentially be influenced by means of fear appeals. We deliberately use the word 'potential' here, because although some of the group differences were significant, the effect sizes were small. A possible explanation is 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. Our results show that 60.1% of the participants reported to have good knowledge of phishing and know what to do against it. Additionally, more variation might have been found if 7-point scales were used.

Because our study took place within participants' social context, we created a realistic setting in which Internet users read the fear appeal and answered questions about their cognitions and behaviours. However, this means that we could not control for the effect of other messages related to safe online practices which were not part of intervention, but which participants may have encountered in their day-to-day use of the Internet. To rule out potential threats to internal validity but also external validity, future studies could adopt a randomized Solomon four-group design (Dimitrov and Rumrill, 2003).

Both a strength and a weakness of the current study is that it focussed on one type of behaviour, as precautionary online behaviour (against phishing) consists of a range of behaviours (Crossler *et al.* 2017). The strength is related to the fact that predictors of one type of behaviour might not influence another type of behaviour (Blythe *et al.* 2015). Therefore, we now have a better understanding of what motivates end users to perform specific individual behaviour. A weakness is that it does not represent precautionary online behaviour as a whole. Rather it studies a type of precautionary behaviour in isolation, possibly hindering the theoretical development of the overall structure of preventing phishing (Posey *et al.* 2015). We did, for example, not focus on recognizing phishing e-mails or phishing websites. Indeed, phishing is a problem that cannot be solved by a single solution at one level (Purkait, 2012). On the other hand, recent research continues to demonstrate that identifying phishing attempts is an extremely difficult task for Internet users (Alsharnouby *et al.* 2015). An important point of discussion for behavioural-information security researchers is whether research on precautionary online behaviour should focus on a single behaviour or on multiple behaviours. Crossler *et al.* (2017) strongly advise to focus on multiple

behaviours concurrently; however, this may make the research designs very demanding for research participants.

6. 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.

7. References

Alsharnouby, M., Alaca, F. and Chiasson, S. (2015), "Why phishing still works: User strategies for combating phishing attacks", *International Journal of Human-Computer Studies*, Vol. 82, pp69–82.

APWG (2015), "Phishing activity trends report: 4th quarter 2014". *Retrieved via: http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf*.

Arachchilage, N.A.G., Love, S. and Beznosov, K. (2016), "Phishing threat avoidance behaviour: An empirical investigation", *Computers in Human Behavior*, Vol. 60, pp185–197.

Blythe, J.M., Coventry, L. and Little, L. (2015), "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors", *Proceedings of the 11th Symposium on Usable Privacy and Security*, pp103–122.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S. and Cotten, S. (2015), "Determinants of online safety behaviour: Towards an intervention strategy for college students", *Behaviour & Information Technology*, Vol. 10, No. 34, pp1022–1035.

Cohen, J. (1988), *Statistical power analysis for the behavioural sciences*, Mahwah, NJ: Lawrence Erlbaum, ISBN: 978-0-80580-283-2.

Crossler, R.E., Bélanger, F. and Ormond, D. (2017), "The quest for complete security: An empirical analysis of users' multi-layered protection from security threats", *Information Systems Frontiers*, pp1–15.

Dimitrov, D.M. and Rumrill, J.P.D. (2003), "Pretest-posttest designs and measurement of change", *Work: A Journal of Prevention, Assessment and Rehabilitation*, Vol. 20, No. 2, pp. 159–165.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 2, pp407–429.

Furnell, S.M., Bryant, P. and Phippen, A.D. (2007), "Assessing the security perceptions of personal Internet users", *Computers & Security*, Vol. 26, No. 5, pp410–417.

Henseler, J., Ringle, C.M. and 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, pp277–320, ISBN: 978-1-84855-468-9.

De Hoog, N., Stroebe, W. and De Wit, J.B. (2005), "The impact of fear appeals on processing and acceptance of action recommendations", *Personality and Social Psychology Bulletin*, Vol. 31, No. 1, pp24–33.

Jansen, J. and Leukfeldt, R. (2015), "How people help fraudsters steal their money: An analysis of 600 online banking fraud cases", *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust*, pp24–31.

Jansen, J. and van Schaik, P. (2017), "Comparing three models to explain precautionary online behavioural intentions", *Information & Computer Security*, Vol. 25, No. 2, pp165–180.

Johnston, A.C., Warkentin, M. and Siponen, M.T. (2015), "An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric.", *MIS Quarterly*, Vol. 39, No. 1, pp113–134.

Lastdrager, E.E. (2014), "Achieving a consensual definition of phishing based on a systematic review of the literature", *Crime Science*, Vol. 3, No. 1, pp1–10.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19, No. 5, pp469–479.

Milne, S., Sheeran, P. and Orbell, S. (2000), "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 1, pp106–143.

Norberg, P.A., Horne, D.R. and Horne, D.A. (2007), "The privacy paradox: Personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, Vol. 41, No. 1, pp100–126.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders' motivation to protect organizational information assets", *Journal of Management Information Systems*, Vol. 32, No. 4, pp179–214.

Purkait, S. (2012), "Phishing counter measures and their effectiveness - Literature review", *Information Management & Computer Security*, Vol. 20, No. 5, pp382–420.

Ringle, C.M., Wende, S. and Will, A. (2005), "SmartPLS 2.0.M3.", *Hamburg: SmartPLS. Retrieved via: http://www.smartpls.com*.

Rocha Flores, W., Holm, H., Svensson, G. and Ericsson, G. (2014), "Using phishing experiments and scenario-based surveys to understand security behaviours in practice", *Information Management & Computer Security*, Vol. 22, No. 4, pp393–406.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91, No. 1, pp93–114.

Sheeran, P., Harris, P.R. and Epton, T. (2014), "Does heightening risk appraisals change people's intentions and behavior? A meta-analysis of experimental studies.", *Psychological Bulletin*, Vol. 140, No. 2, p. 511–543.

Witte, K. (1992), "Putting the fear back into fear appeals: The extended parallel process model", *Communications Monographs*, Vol. 59, No. 4, pp329–349.

Witte, K. and Allen, M. (2000), "A meta-analysis of fear appeals: Implications for effective public health campaigns.", *Health Education & Behavior*, Vol. 27, No. 5, pp591–615.

Witte, K., Berkowitz, J.M., Cameron, K.A. and McKeon, J.K. (1998), "Preventing the spread of genital warts: Using fear appeals to promote self-protective behaviors", *Health Education & Behavior*, Vol. 25, No. 5, pp571–585.