International Journal of Human-Computer Studies 123 (2019) 29–39

Contents lists available at ScienceDirect

International Journal of Human-Computer Studies

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

Using protection motivation theory in the design of nudges to improve online security behavior

René van Bavel[a,*], Nuria Rodríguez-Priego[a,d], José Vila[b], Pam Briggs[c]

[a] Joint Research Centre, European Commission, Edificio Expo, C/ Inca Garcilaso 3, Sevilla (41092), Spain
[b] DevStat Chair on Quantitative Decision-making and Intelligent Data Analysis Laboratory, Center for Research in Social and Economic Behavior, University of Valencia, Spain
[c] Department of Psychology, School of Life Sciences, Northumbria University, Northumberland Building, Newcastle upon Tyne, NE1 8ST, United Kingdom
[d] Universidad Autónoma de Madrid, Departamento de Análisis Económico: Teoría Económica e Historia Económica, Campus de Cantoblanco, 28049, Madrid, Spain

ARTICLE INFO

Keywords:
Security behavior
Protection motivation theory
Behavioral economics
Online experiment
Coping message
Threat appeal
Nudging

ABSTRACT

We conducted an online experiment (n = 2024) on a representative sample of internet users in Germany, Sweden, Poland, Spain and the UK to explore the effect of notifications on security behaviour. Inspired by protection motivation theory (PMT), a coping message advised participants on how to minimize their exposure to risk and a threat appeal highlighted the potential negative consequences of not doing so. Both increased secure behavior – but the coping message significantly more so. The coping message was also as effective as both messages combined, but not so the threat appeal. Risk attitudes, age and country had a significant effect on behavior. Initiatives seeking to promote secure behavior should focus more on coping messages, either alone or in combination with fear appeals.

1. Introduction

Digital technology has enabled innovation, greater connectedness, economic growth and productivity, but has also given rise to the threat of cybercrime. Criminal adversaries now have access to a range of resources to support cyberattacks, many of these becoming more widely available, such that nearly half of organizations surveyed in a 2017 report had been subject to serious cyberattacks, many as a consequence of social engineering attacks. Users are aware of this threat and many now shy away from certain activities over the internet (especially those that involve the disclosure of personal information or economic transactions), yet a majority of security professionals report concerns about the behavior of end users and would seek measures to change or limit vulnerable behaviors such as clicking malicious links in emails (Cisco, 2017).

In Europe, a report has shown that 27% of users are reluctant to use the internet for e-commerce transactions due to concerns about the lack of security in online payments (Cisco, 2017; European Commission, 2016). In a survey in the United States in 2017, 64% of Americans reported that they had personally experienced a major data breach, with 41% having reported fraudulent charges on their credit cards and 35% reporting that sensitive data (such as an account number) had been compromised. Not surprisingly, nearly half of Americans (49%) feel that their personal information is less secure than it was five years ago (Pew Research Center, 2017).

For many years, researchers and security professionals have reported that the 'weakest link' in any security chain is human behavior. Indeed, social engineering attacks are now commonplace and considered one of the most significant threats to organizations and users alike (Cisco, 2017). Nearly one-quarter of all cybersecurity failures are due to human error (Waldrop, 2016). Certainly, with the rise of social media, human vulnerabilities have escalated as information posted online can be used to identify potential victims (Saridakis et al., 2016; Shelton and Skalski, 2014). However, many researchers recognize that it is unreasonable to simply cite 'human error' as a major factor without first understanding that users are 'not the enemy' (Adams and Sasse, 1999). Users are simply faced with overly complex security systems, unusable cybersecurity policies and a complex range of other job demands than mean that they lack the knowledge, the time and the support to be able to deal with cyber threats (Kraemer et al., 2009). As a result of such insights, 'usable security' is now seen as a key issue in the design of more resilient systems (e.g. Herley, 2014).

There are significant challenges, therefore, in ensuring that people are both aware of cybersecurity risks and can respond to those risks in a meaningful way. Simple policy campaigns or warning messages, intended to increase their awareness of the risks involved are not always

* Corresponding author.
E-mail address: rene.van-bavel@ec.europa.eu (R. van Bavel).

https://doi.org/10.1016/j.ijhcs.2018.11.003
Received 29 November 2017; Received in revised form 7 September 2018; Accepted 2 November 2018
Available online 03 November 2018

effective, as they implicitly rely on users making very informed or rational decisions (Acquisti et al., 2015). Also, users find it relatively easy to dismiss the threat as irrelevant or unlikely, or they fail to act, simply because they have neither the time nor the skills to respond (Bulgurcu et al., 2010; Reid and Van Niekerk, 2016).

Unfortunately, hackers seem to be more knowledgeable about human behavior and exploit this knowledge via sophisticated social engineering attacks. They send phishing emails from a sender that seems authoritative, at a time of the day when users are busy, increasing the chances that they will click where they should not. The institutions meant to defend users, on the other hand, are lagging behind. The excessive requests for authentication in an organization (23 per day on average, according to a study by Stevens et al., 2014), drain people's time and mental energy and recent evidence suggests that the guidelines for proper password management are misguided (Waldrop, 2016). The end result is a series of onerous initiatives that work to increase the security 'compliance budget' (Beautement et al., 2009; Bulgurcu et al., 2010).

Recently, the focus has turned towards a more human-centered perspective on cybersecurity. Towards the end of his time in office, President Obama proposed spending more than $19 billion in federal cybersecurity funding, including a research and development plan that made human-factors research an explicit priority. Similar trends were found in the UK (e.g. with research funding for a large 'human-dimensions of cybersecurity' initiative made in 2016). Research outcomes that place usable security at the heart of business include the promotion of more usable passwords (National Cyber Security Centre, 2016; Waldrop, 2016) and a range of new guidelines and frameworks designed around user behavior (Briggs et al., 2017; Nurse et al., 2011).

This article follows that trend. It is part of a larger initiative which takes a human centred approach to cybersecurity and explores the contribution of behavioral insights to cybersecurity. The aim is to observe whether small changes in the design of online notifications (i.e. a *nudge* according to the behavioral economics literature; Thaler and Sunstein, 2008) can seamlessly trigger more secure behaviors.

Our study is based on an online experiment (n = 2024) across five European countries: Germany, Sweden, Poland, Spain and the UK. We randomly assigned participants to a control group or one of three treatment groups, and then let them purchase in a mock e-commerce store. The nudges applied were subtle, and were embedded in a notification reminding them to navigate safely. They differed across treatment groups in how they directed participants' attention, and were based on insights from protection motivation theory (PMT).

2. Protection motivation theory

PMT seeks to clarify the cognitive processes which mediate behavior in the face of a threat (Rogers, 1975, 1983). It posits that, when facing a threatening event, people conduct two appraisal processes: one focused on the threat itself and the other on their ability to act against that threat (threat appraisal and coping appraisal, respectively). This affects their intention to take precautionary action and results in adaptive or maladaptive behaviors vis-à-vis the threat.

In their threat appraisal, people will consider how negative the consequences of the threat are (perceived severity) and the likelihood of the threat materializing in a way that will affect them directly (perceived vulnerability). This threat appraisal may lead to maladaptive behaviors such as denial or avoidance (e.g. Witte and Allen, 2000). In their coping appraisal, people will assess whether undertaking a recommended course of action will remove the threat (response efficacy) and also their level of confidence in being able to carry that action out (self-efficacy; Boer and Seydel, 1996; Maddux and Rogers, 1983; Bandura, 1997). This appraisal my lead to adaptive behaviors, providing that the costs of making an adaptive response (response costs) are not too high. In two meta-analyses of the traditional PMT literature, largely taken from studies in the health domain, the coping appraisal components had larger effect sizes than the threat appraisal components on both behavioral intentions and actual behaviors. In addition, the effect sizes for intentions were greater than for behaviors (Floyd et al., 2000; Milne et al., 2000).

PMT has been applied to cybersecurity, specifically to virus protection behavior (Lee et al., 2008), security behavior among people who know how to protect their systems but fail to do so (Workman et al., 2008), security behavioral intentions of home computer users (Anderson and Agarwal, 2010), convincing internet users to protect themselves (Shillair et al., 2015), the role of personal responsibility in the protective behavior of college students (Boehmer et al., 2015); teenagers' willingness to provide information online (Youn, 2005), security behavior in response to fear appeals by employers (Johnston and Warkentin, 2010), and employees' adherence to information security policies (Ifinedo, 2012; Siponen et al., 2014). An analysis of the effect sizes of these various constructs in the cybersecurity literature was recently conducted by Mayer et al. (2017) who concluded that all PMT constructs aside from 'response cost' had reliable positive albeit weak to medium effect sizes. Response costs on the other hand, had weak to strong negative influences on cybersecurity.

There is, therefore, a significant and growing body of research in this area, however most of the PMT studies have used *behavioral intention* as a proxy for cybersecurity behavior. This is typical of many approaches that are derived from Ajzen's (1985) theory of planned behavior, which has behavioral intention as the primary driver of observed behavior. But while behavioral intentions are generally quite well correlated with subsequent behaviors, there is a known gap between intention and behavior (Sheeran, 2002; Sniehotta et al., 2005). A review of the evidence suggests that intentions result in behavior only about half of the time (Sheeran and Web, 2016). This is a limitation of the studies that have used PMT as an explanatory model in the cybersecurity sphere (e.g. Boehmer et al., 2015; Crossler et al., 2014; Herath and Rao, 2009; Johnston and Warkentin, 2010; Lee, 2011; Liang and Xue, 2010; Tsai et al., 2016).

A few studies have used actual behavior as the dependent variable (Neuwirth et al., 2000; Woon et al., 2005; Workman et al., 2008), which works better than intention. When it comes to privacy and security behavior, protection of information resources relies upon action rather than intention (Crossler et al., 2013). However, even in those studies where behavior is the dependent variable, self-reported behavior is often used as a proxy measure (e.g. Crossler et al., 2014) and there are questions about how reliable such measures are. In contrast, the current study captured behavior in an incentivised experiment, also adopting a sample size that far outstrips most of those studies based on behavioral intention and reported behavior. This then constitutes one of the greatest strengths of this study and ensures a distinct contribution to the field.

The premise of the current study is that people will behave more securely online if (a) their awareness of the threat is heightened (threat appraisal) and (b) they are made aware of the appropriate protective responses to take (coping appraisal). To explore this, we set up a task in which participants were asked to navigate an e-commerce site securely. Three PMT-inspired notifications were designed to trigger or nudge more secure behavior:

- A *coping* message told users it was easy to minimize the chances of a cyber-attack and also indicated what steps to take.[1]
- A *fear appeal* warned individuals that their behavior could leave them vulnerable to a cyber-attack.
- A *threat and coping* message contained both elements described above.

[1] This is similar to a persuasive boost in self-efficacy, one of four sources of self-efficacy according to Bandura (1997), in addition to mastery experience, vicarious experience and physiological factors.

The threat appeal highlighted both the severity of the threat and the user's vulnerability at the same time, since prior research (outside security behavior) suggests they jointly determine the likelihood of individuals performing adaptive behaviors (Neuwirth et al., 2000). Taken together, these three messages drove the following hypotheses:

Hypothesis 1. The group exposed to the coping message will show more secure online behavior than the control group.

Hypothesis 2. The group exposed to the threat appeal will show more secure online behavior than the control group.

Hypothesis 3. The group exposed to the combined coping + threat message will show more secure online behaviour than the control group.

We were also interested in which of the threat vs coping messages would be more effective and also whether the threat and coping elements would be additive (i.e. to explore whether the two elements combined would be more effective than each presented in isolation) – but here our expectations here were less clear. From the survey literature, there is some evidence that coping messages are stronger predictors of good security behaviors than threat appeals (e.g. Shillair and Dutton, 2016), yet we were also mindful that there is a response cost to taking 'coping' actions which may possibly act to deter participants in the coping and threat + coping conditions. It is interesting, too, to note that in the much more extensive literature on health behavior change, strong fear appeals when presented alone have been deemed ineffective (generating high levels of defensive responding without corresponding action), whereas strong fear appeals presented in combination with coping messages have produced the greatest behavior change, despite the associated response costs (Witte and Allen, 2000).

Finally, while we might anticipate the main effect of manipulating threat appeals and coping information across our participant sample, it is worth considering whether these interventions are likely to be mediated by other factors. For example, we know that older adults show some distinct vulnerabilities. They are more suspicious about online security threats, feel overwhelmed by their changing nature, do not feel they can cope with them, implement fewer coping strategies in their defense, and are more likely to rely on others for assistance (Grimes et al., 2007; Jiang et al., 2016; LaRose et al., 2015). They are also more willing to trust those they encounter through digital transactions (Grimes et al., 2010) and so it is not surprising that they are disproportionately targeted for internet crime and fraud (Martin and Rice, 2013). For this reason, it is worth considering the age of the participant as an important variable in this study.

Another important issue is the extent to which any individual might tolerate risk. The Domain-Specific Risk-Taking (DOSPERT) scale measures self-reported propensity to engage in risky behaviors across ethical, financial, health and safety and social behaviors. Although this is a general measure of risk-taking propensity it has good psychometric properties and been used quite widely in cybersecurity research (see Gratian et al., 2018; Hadlington, 2018; and Tischer et al., 2017 for recent examples). It has been shown to predict the extent to which an individual might engage in security behaviors such as visiting untrusted sites (Egelman and Peer, 2015a). Such scales can be used for the psychographic targeting of privacy and security interventions and it is worth exploring the way that personal propensity to risk might moderate the uptake of any intervention designed to help people be safe online (Egelman and Peer, 2015b).

3. Materials and methods

3.1. Participants

A total sample of 2024 participants, evenly distributed across Sweden, Poland, Germany, Spain and the UK, were recruited through the Toluna online panel.[2] Toluna recruits members for its proprietary panels using various methods including web-banners, website referrals, pay-per-click, natural search optimization, affiliate marketing, email, and online public relations activities. In addition, Toluna applies *Real-Time Sampling®* to recruit individuals in real-time from a network of websites with which Toluna has developed referral relationships. This methodology taps into the many potential survey takers online who are willing to participate in surveys, but who may not necessarily want to join a market research panel. Past-participation and participation frequency is limited by tracking each respondent's participation over the full duration of the study. The panel applies a points-based incentive system that, in the case of our economic experiment, included both a fixed participation fee and a variable incentive depending on participants' decisions and random events that may take place during the experiment. Toluna uses techniques for monitoring and limiting fraudulent respondents through active cleaning and exclusion of observed offenders from the panel. Sample selection[3] was made randomly among panellists that had bought a good or service online in the last 12 months. Sex and age quotas were established for each combination of experimental condition and country. Each experimental treatment group included at least 100 participants from each country. Panellists were invited to participate in the study once, with no further follow up. The Ethics Committee on Experimental Behavioural Economics at the Center for Research in Social and Economic Behavior (ERI-CES), University of Valencia, approved the experiment and confirmed that it adhered to its charter of ethics. Informed consent was given by all participants.

3.2. Procedure

The overall design of the experiment was simple: participants had to navigate as securely as possible while making a mock online purchase of a digital good on an e-commerce website. The more secure their behavior, the lower was their probability of a suffering a cyber-attack (which was the main outcome measure) and the higher their probability of receiving a variable fee in addition to a fixed fee.[4] Secure behavior also typically incurs a higher 'response cost' in terms of time and effort to complete the study, which may have mitigated the effect of the payoff (see Briggs et al., 2017). However, this was the same for all treatments, i.e. there was no independent manipulation of response costs across treatments. Note our use of an e-commerce simulation was a variant of the 'free simulation methodology' described by Gefen and Straub (2004) in which participants are presented with e-commerce web pages highly similar to those found in real-world settings. Note also that in keeping with the free-simulation methodology and to ensure good ecological validity, there were no experimental manipulations of the web pages themselves across treatments. The treatment manipulations appeared in a pop-up message immediately after the participant entered the e-commerce environment.

Participants from the online panel were invited to the experiment in an email message sent by Toluna. To participate they had to click on a

[2] A detailed description of the recruitment sources and procedures applied by Toluna, as well as a description of its quality controls and standards and their privacy and ethics policy can be found at www.toluna-group.com/docs/default-source/Brochure_Docs/esomar-28.pdf?sfvrsn=10 validation methods and data protection.

[3] This sample was extracted from a larger sample of 5,065 participants across those same countries, which included additional experimental treatments not covered in this article (van Bavel and Rodríguez-Priego, 2016).

[4] The use of a variable economic incentive to generate induced value is a differential feature of economic experiments. Through the variable fee, participant's decisions have an actual impact, increasing the ecological validity and the accuracy of the experimental results. For a detailed discussion see Smith (1976) and Holt and Laury (2002).

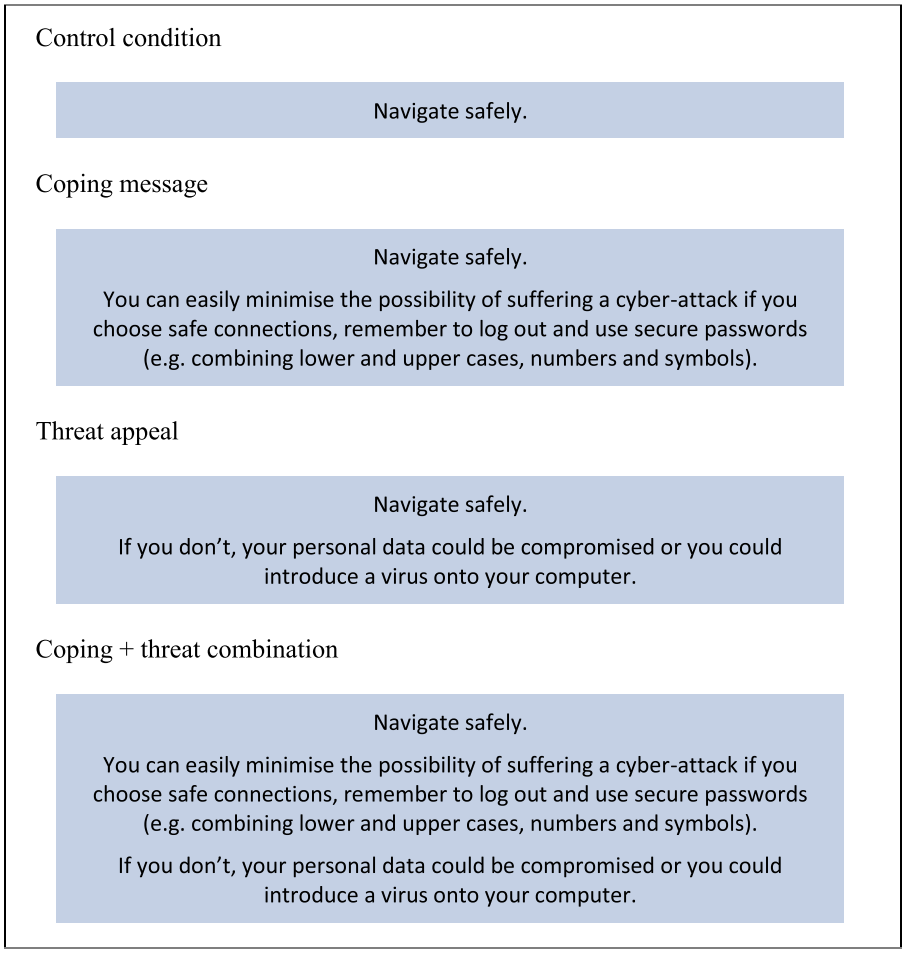

Fig. 1. The four security notifications tested.

link. Participants were familiar with Toluna and their recruitment practices, and had voluntarily given them their contact details. Therefore, despite the risk of phishing attacks through emails containing hyperlinks from an alleged known sender (Vishwanath et al., 2018), no distrust in Toluna's email or embedded link was expected in this case. At the initial screen they had to report their age and gender to comply with the quotas for representativeness according to these variables. They were then shown the general instructions for the experiment, which included information about secure behavior and the additional variable payment. Subjects did not have information at this stage on how much variable payment they would receive. They were only informed about the need of navigating safely during the experiment or they would increase the probability of suffering a cyber-attack, which would result in receiving less variable payment at the end. Every time they made a decision that was not safe, the probability of a cyber-attack increased.

Before the mock purchasing process began, participants answered questions relating to their socio-demographic characteristics and the DOSPERT scale (Blais and Weber, 2006; Weber et al., 2002). As soon as the purchasing process began, participants were exposed to a notification of the risks of unsecured behavior (based on insights by PMT, Fig. 1). The objective of the experiment was to observe if this message, which varied across experimental treatments, affected the level of security of participants' online behavior.

During the purchasing process, participants had the opportunity of taking four security-related actions. These were actions that are considered necessary for users to maintain cybersecurity (Coventry et al., 2014). Participants' choices at these points in the purchasing process determined their overall level of secure behavior.

3.2.1. Action 1: choosing a secure connection

Participants had to connect to a simulated intranet before entering the eCommerce website. They faced a choice: spend extra time and effort connecting securely or select an instant connection which left them exposed (Figure A2, Appendix A). This setup was designed to reflect the costs of secure behavior. It sought to evoke the *compliance budget* that users resort to when making a decision (Beautement et al., 2009), i.e. the selection of a secure connection incurs a response cost.

The secure connection implied waiting for 60 seconds and entering a lengthy access code which combined 12 upper- and lower-case letters and numbers (such as eH2GdR56Mb9A). The unsecured connection, on the other hand, meant an instant connection and did not require a password. If participants chose the secure option, the next screen displayed a processing bar while the connection was established. Below the bar was a button that allowed participants to switch to the unsecured connection, in case they became impatient (as in the real world). Participants scored zero if they chose not to behave securely and one if they made the secure choice.

3.2.2. Action 2: selecting a trusted vendor

In the eCommerce website, once a product was selected, a detailed product information page appeared. On this page, there was a choice of two vendors, which appeared in random order (Figure A3, Appendix A). One vendor offered the product for free through a Hypertext Transfer Protocol, or HTTP, link. The other vendor offered the product for €2 through a Hypertext Transfer Protocol *Secure* link, or https, with a logo next to it suggesting the link could be trusted. Participants scored zero if they chose the unsecured option and one if they chose the secure option (i.e. the trusted vendor). This set-up (or *choice architecture* in the

behavioral economics nomenclature) sought to reflect how, in the real world, access to free products through unknown sites may imply a security risk, which is mitigated when a product is purchased through a trusted vendor.

3.2.3. Action 3: choosing a strong password

Participants had to create their passwords when registering on the eCommerce site. On the same screen, participants were asked to introduce the number, CVV and expiry date of a simulated credit card shown (see Figure A4, Appendix A). A poor password was taken as an indicator of unsecured behavior.

A secure password adhered to six security criteria, which included a minimum number of characters (in total), lower case characters, upper case characters, numeric digit characters, and special characters. A final criterion was that the password should not contain the username. Participants scored between zero (if they did not meet any of the criteria) and six (if they met them all).

3.2.4. Action 4: logging out

Once subjects had completed the purchasing process, a button appeared at the bottom right-hand side of this screen which led participants to the 'next questionnaire'. However, they had the option to log out before doing so, by clicking on a button in the top right-hand corner (see Figure A5, Appendix A). Logging out of their eCommerce session was considered secure behavior, but the website did not specifically ask participants to log out. It simply asked them to exit the eCommerce site and complete the second questionnaire. Participants scored zero if they just clicked on the 'next questionnaire' button and one if they chose the safe option and logged out first.

3.3. Main outcome measure

The main outcome measure of this study was the probability of the participant to suffer a cyberattack in the experiment, which would reduce her or his variable payment. This probability was a continuous value from 5% to 65%, determined by the decisions made by participants during the experiment. Specifically, the minimum probability of suffering the cyberattack in the experiment was set at 5%. From this minimum value, the selection of an unsecured connection, a non-trusted vendor or not logging out added up to the probability of cyberattacks by 15 percentage points each. Finally, lack of strength of the selected password added up to this probability on a range from zero percentage points (if the password met all six security criteria[5]) to 15 points (if it met none).

The probability of suffering the attack worked as a measure of the security level of decisions made by the subjects: if they always proceeded in the safest way this probability was kept at its minimum value (5%). On the other hand, if a subject selected the riskiest option at each step of the experiment, the probability reached its maximum value (65%). This maximum probability was much higher than what could be expected when navigating well-known e-commerce sites in the real world. This was done to offer a wide range of variation in the outcome measure. Also, since this value was actually not known by participants, it had no impact on their online behaviour. Finally, although the probability of suffering a cyberattack was not related to the actual chances of suffering a cyberattack outside the experiment, the decisions that determined the probability were based on good security behaviour in the real world (Coventry et al., 2014).

[5] The six security criteria for the password are: non-inclusion of the user name as part of the password; length of at least 8 characters; and inclusion of at least two lower-case, upper-case, numerical, and special characters, respectively.

3.4. Experimental treatments

The experimental treatments were based on a notification which appeared as a pop-up window in the centre of the screen at the beginning of the purchasing process. Participants had to close it in order to continue with the experiment. The message then appeared in the upper part of the screen and remained there throughout the purchasing process. Participants were randomly assigned to either the control or one of three treatment groups. The samples sizes were almost identical for each experimental condition (as shown in Table 2, the smallest sample size was 504 subjects and the largest sample size 508). No procedure to compensate potential differences in samples sizes was required.

In the control condition, the message simply reminded the participant to navigate safely. The experimental conditions, based on PMT, sought to heighten self-efficacy and response efficacy (both components of coping appraisal) and perceptions of the cybersecurity threat. The warning messages are presented in Fig. 1. Six other treatments were included in the larger study which provided the data for this article; however, only the treatments related to PMT are reported here.

4. Results

This section presents a brief discussion of the socio-demographic profile of participants in the sample, including the possible impact of dropouts (i.e. people who began the experiment but did not complete it) on the final sample. Following this, the section analyses the effects of the different treatments using an ANCOVA model.

4.1. Sample profile

The final sample of participants in the experiment was representative regarding sex and age of the national population that had bought goods or services online in the last 12 months. These quotas, different for each country, were applied equally to the four treatment groups in each country. In the total sample, 50.3% of the participants were women and the mean age was 40.8 years. The educational level and employment status of the participants are shown in Table 1.

The sample consisted of participants who volunteered to complete the online experiment. In this context, the number of dropouts merited close attention, as it could have affected the results of the experiment. Naturally, given data protection and consent practices, no information is available on dropout demographics immediately following the invitation to participate in the experiment (as there was no consent to collect data). However, it is worth noting that dropouts at this point could not reflect any effect of treatment as participants did not yet fully understand the nature of the experiment. Our analysis of dropouts dealt with three subsequent stages of the experiment, the most critical point being the moment when the warning message was shown (21.8% of the dropouts). Dropouts were also significant at the sign-up stage, where (mock) payment data were required (13.1%) and at the presentation of instructions on how to proceed with the mock online purchase (11.2%). In other words, the main triggers of dropouts were the messages increasing the awareness of cybersecurity problems and those points in the experiment where participants were interacting with a mock e-commerce site, which they may have mistrusted. The percentage of dropouts varied from country to country, from the minimum level in Spain (49.8%) up to the maximum level in the UK (73.2%). The dropouts in Poland, Sweden and Germany were 66.6%, 66.9% and 72.9%, respectively.

Warning messages about cyber-security threats may have dissuaded people from continuing with the experiment instead of increasing the security of their online behavior, but here the dropouts according to treatments is interesting.

The threat appeal led to the largest number of dropouts (65.3%), followed by the coping + threat combination (61.4%) and the coping

Table 1
Education level and employment status of participants.

Education level	%	Employment status	%
No studies	0.35	Self-employed	8.16
Primary or lower secondary education	12.51	Employed by a public or private institution	53.51
Upper secondary education and post-secondary, non-tertiary education	40.84	Unemployed	9.11
Bachelor degree or equivalent	33.95	Homemaker	4.63
Postgraduate degree	12.35	Student	10.35
		Disabled	4.13
		Retired	9.51
		Other	0.6

message (61.5%). The control condition showed a dropout rate of 58.2%. The difference between the threat appeal and the control condition is significant ($t = 2.29$, $p < 0.05$), but not so the differences between the other two treatment groups and the control. In the light of these results, we controlled for the possibility that dropouts led to a biased sample: i.e. those participants who were most affected by the warning messages might have dropped out, leaving the more resilient or blasé individuals to complete the experiment. We checked this by analyzing the risk appetite of both groups (using the DOSPERT scale). Using a *t*-test, we compared (a) drop-outs with (b) subjects completing the experiments, without the assumption of equality of variances for each item between both groups. In the control group, we detected no difference in DOSPERT scores between dropouts and non-dropouts (*p*-value = 0.251). However, we observed differences between these groups in the other three treatments (*p*-value = 0.003, 0.043 and 0.004 for threat, coping and coping + threat treatments, respectively).

The results suggest that notifications had an impact on the type of person who dropped out: the more risk-averse tended to drop out following the warning, while the more risk-seeking tended to stay. To control for this effect in subsequent analyses, DOSPERT scores were included as variables in the model testing the effect of warning messages on behavior.

4.2. Effects of the treatments on the main outcome measure

The calculated probability of suffering a cyberattack differed across treatment groups, being highest in the control group and lowest in the coping message and coping + threat combination groups (Table 2 and Fig. 2). Table A3 in Appendix A breaks down the effect of the treatments on the different behaviors that determined the probability of suffering a cyberattack. By performing an a priori hypothesis test (specifically a Kruskal-Wallis test that can be considered a non-parametric version of ANOVA), we can reject the null hypothesis that the median of the probability of suffering an attack is identical in the four experimental conditions. The test statistic, which is distributed as a Chi square with 3 degrees of freedom, is 72.63 with a *p*-value smaller than 0.001.

Since probabilities are continuous variables, the most appropriate method to estimate the effect of the notifications is an analysis of covariance (ANCOVA). The application of an ANCOVA model requires some statistical assumptions: the sample size for the control and the treatment groups needs to be similar (balanced samples), the sampling distribution of the mean of the dependent variable has to be normal (normality assumption), and its variance has to be the same among the four experimental conditions. As shown in Table 2, the sample sizes are almost identical in the four experimental conditions. On the other hand, the Central Limit Theorem states that given random and independent samples of N observations each, the distribution of sample means approaches normality as the size of N increases, regardless of the shape of the population. Given the size of the total sample (2024 cases), we use this asymptotic property to assume normality, although this is a limitation of the model since our data have been obtained by quota sampling. Hypothesis testing is not an adequate tool to use to assess the validity of the assumption of equality of variances among experimental treatments. If the sample size is small, they have no power to detect any variance differences, even if the variance differences are large. If the sample size is large (as in this case), tests have enough power to detect even the most trivial deviations from equal variance, and the null hypothesis of equal variance will be rejected. This situation is observed in our case: Table 2 shows that the standard deviations in the control and in each of the three treatments are similar, although the Levene test for equality of variances rejects the null hypothesis of equality of variance among the different experimental conditions ($F = 3.08$, *P*-value = 0.00).

Table 2
Mean and standard deviation of the probability of suffering a cyberattack by treatment group (%).

Group	Sample size	Mean	Standard deviation
Control	507	34.41	13.33
Coping message	505	28.11	15.33
Threat appeal	504	31.44	12.32
Coping + threat combination	508	28.03	14.54

We estimated a first ANCOVA model with (i) the probability of suffering a cyberattack as the dependent variable; (ii) the three PMT treatments (coping message, threat appeal and coping + threat combination) as independent variables and the control condition as a baseline; (iii) age, sex, risk aversion and country as independent control variables; and (iv) the interactions between control and treatments included. This first ANCOVA showed no significant impact of sex. Moreover, the model presented no significant interaction between the control variables and treatments, showing that the effect of the treatments do not depend on the age, sex, risk aversion or country of residence of participants. We eliminated these non-significant variables and conducted a final ANCOVA (Table 4). This final model can explain the probability of cyberattack (*F*-statistic = 14.09 with a *p*-value < 0.001) and can be applied to analyze the effects of the treatments. Table 3 presents the detailed Analysis of Variance of the final model. This table shows the results of the tests of the impact of country, age and risk attitude, as well as the impact of the experimental treatments. The results of the corresponding F-tests (*P*-values ≤ 0.001) suggests all these factors are significant and should be considered in the model. As discussed before, the size of the sample is large, which makes the statistical test prone to reject the null hypotheses. To provide a clearer view of the actual explanation level provided by each variable, Table 3 also presents the values of the variance explained by each variable (η^2).

The estimation of the final model is presented in Table 4. As shown by the corresponding statistical test (*p*-value < 0.001), all experimental treatments had a significant impact on participants' behavior, reducing their probability of suffering a cyberattack. Again, due to the large sample size, it is convenient to state not only the *p*-value, but also information on the actual values of the effects of the treatments on the probability of suffering the cyberattack. This information is provided by the estimated values of the coefficients in Table 4, which shows that cyberattack probability is reduced by 6.32% (coping message), 3.12% (threat appeal) and 6.51% (coping + threat message), respectively. Research hypotheses 1 to 3 are supported by our data.

Post-hoc analysis with a Tukey test compared the difference in probability of suffering a cyberattack between pairs of experimental groups. Fig. 3 presents the confidence intervals for these differences (if zero is included in a given interval, the average probability was the same, at a 95% confidence level). There was a difference between all treatment groups and the control group, between the coping message and the threat appeal, and between the coping + threat combination and the threat appeal. However, there was no difference between the coping message and the coping + threat combination.

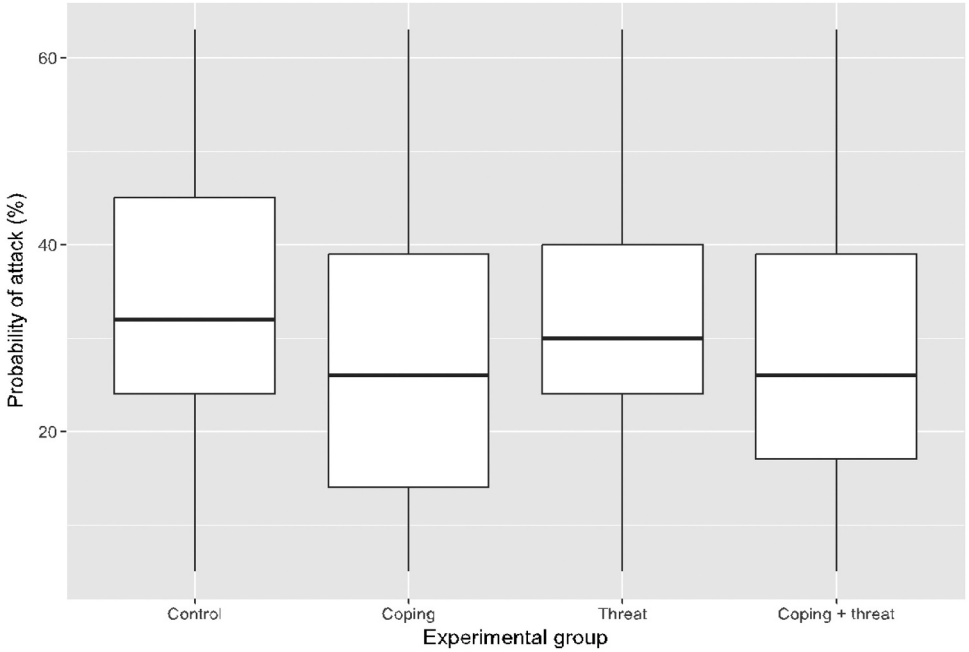

Fig. 2. Box-plot of the probability of suffering a cyberattack by experimental group (%).

Table 3
Analysis of Variance of the final model.

	Df	Sum Sq	Mean Sq	F value	Pr(> F)	η^2
Country	4	4854.00	1213.50	6.40	0.000	0.01
Age	1	2738.80	2738.80	14.44	0.000	0.01
Risk	1	2012.52	2012.52	10.61	0.001	0.01
Treatment	3	14,455.59	4818.53	25.40	0.000	0.04
Residuals	2014	382,055.05	189.70			

Table 4
Estimated coefficients of the final model.

	Estimate	Std. Error	*t* value	Pr(> |*t*|)
(Intercept)	33.55	2.05	16.31	0.000
Germany	−1.18	0.97	−1.20	0.227
Poland	0.05	0.96	0.05	0.952
Sweden	−2.59	0.97	−2.66	0.007
UK	−2.81	0.98	−2.85	0.004
Age	−0.06	0.02	−3.11	0.001
Risk	2.02	0.59	3.40	0.000
Coping	−6.32	0.86	−7.30	0.000
Threat	−3.12	0.86	−3.60	0.000
Copying + threat	−6.51	0.86	−7.53	0.000

In other words, treatments including a coping message worked better than a threat appeal; it was more effective to tell subjects how to effectively manage the probability of suffering a cyberattack than to threaten them with the consequences of not behaving safely. Viewed differently, a coping message was effective and the addition of a threat appeal did not significantly increase its effectiveness (Table 2). On the other hand, although the threat appeal on its own was effective, the addition of a coping message significantly increased its effectiveness.

In addition to the experimental groups, the ANCOVA model included three control variables for subject's profile: age, attitude to risk and country (Table 4). Age had a significant and negative impact on the probability of suffering a cyberattack: the older the participant, the more securely he or she navigated through the mock purchasing process. This does not necessarily indicate a linear relationship and could of course be due to the riskier internet behaviors of younger adults. Indeed the relationship between age and cybersecurity is highly complex. For example, older adults are more vulnerable than younger adults to certain types of phishing attack, but less vulnerable to others (Oliveira et al., 2017). Both younger and older adults are likely to modify their purchasing security behaviors following a warning of some kind but older adults are particularly affected by trust violations (Chakraborty et al., 2016). The effect of age is also likely to be moderated by e-commerce experience, as age effects do not tend to emerge with very experienced e-shoppers (Hernández et al., 2011). Risk attitude, measured with the DOSPERT scale, had a significant and positive impact on the probability of suffering a cyberattack. The more risk-seeking the participant, the higher was his or her probability of suffering a cyberattack.

Finally, about country, the probability of suffering a cyberattack was significantly lower for participants in Sweden and UK than in Spain (taken as the baseline). A Tukey test also looked at the differences between other pairs of countries: they are confirmed for the UK and Spain, the UK and Poland and, to a lower extent, between Sweden and Poland and Sweden and Spain (Fig. 4).

5. Discussion and conclusion

Our first and clearest finding is that those participants exposed to a coping message, either in isolation or in combination with a threat appeal, behaved more securely than participants in the control condition. In other words, the most successful interventions simply involved telling our participants what effective actions to take to protect themselves online. This emphasis on protective coping behaviors is interesting given Schillair et al.'s (2015) observation that the PMT literature has spawned a significant number of studies in relation to the presentation of threat appeals, but that insufficient attention has been given to changing coping appraisals. In taking this argument forward, Burns et al. (2017, p. 193) have claimed that 'security conceptualizations have largely ignored positive coping, such as self-efficacy, and have focused on security motivation purely in terms of fear appeals'.

In the Burns et al. (2017) paper, organizational employees learned how to protect themselves online and then answered a multi-component questionnaire designed to identify the predictors of their intention to engage in those protective behaviors. The authors found the coping

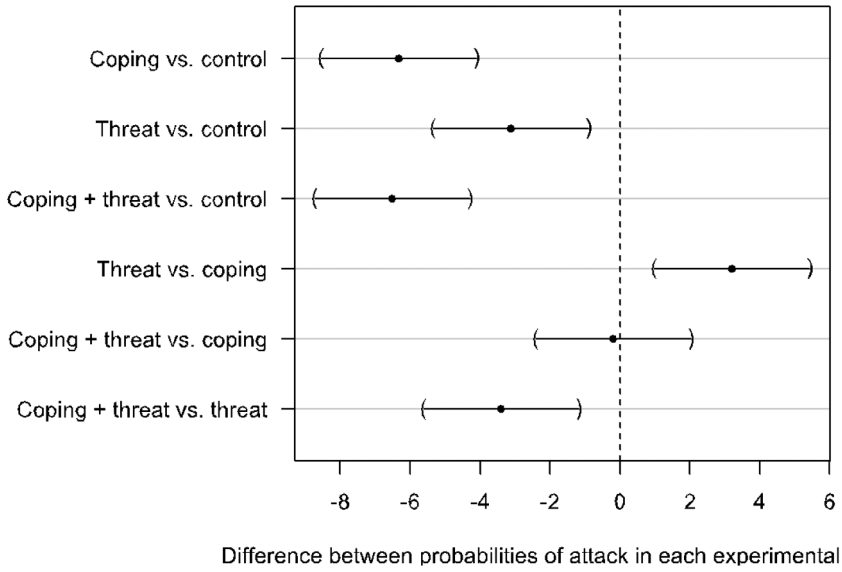

Fig. 3. Confidence intervals for the difference of the average probabilities of suffering a cyberattack between pairs of experimental groups (confidence level: 95%).

elements of PMT were more influential than the threat appeals in predicting *intention* to engage in protective behaviors. In another recent paper exploring security behaviors in the home environment, Hanus and Wu (2016) found again that two of the coping appraisal elements of PMT (self-efficacy and response-efficacy) were significant predictors of *reported* security behavior, while the threat elements (perceived severity and perceived vulnerability) did not predict secure behavior. We should note, however, that both of these studies were based upon survey data, while our study is the first to demonstrate the primacy of coping interventions in a study that captures observed behavior.

Some limitations apply to this study. For one, the observed behavior took place in an experimental setting, where participants were asked to navigate safely through and mock online shopping exercise. While the experiment was incentivised, it did not capture the *actual* behavior of someone dealing with an online threat, which might exhibit different characteristics. The experiment was also conducted online, which means the environment was less controlled than in a lab. For example, participants could have been distracted by background noise or influenced by the presence of other people in the room. This means that other factors, apart from the manipulated variables, could have had a bearing on behavior. Other limitations are a consequence of applying the ANCOVA model in our analysis. ANCOVA models assume that the dependent variable is continuous, normally distributed and homoscedastic. As discussed in Section 3, our dependent variable is constrained to 2.5% increments and cannot take all possible real values. Moreover, although normality is claimed as consequence of the central limit theorem for random sample, the ANCOVA model has been applied to data obtained by quota sampling. As regards homoscedasticity, although the standard deviation of the dependent variable is similar in the four experimental conditions, the Leven test rejects the null hypothesis of the variance being identical in the four groups. Finally, the variance explained by the different independent variables in the model (eta squared) is low and the reliability of the dependent variable of the model is unknown.

We can turn to the wider psychological literature on PMT and

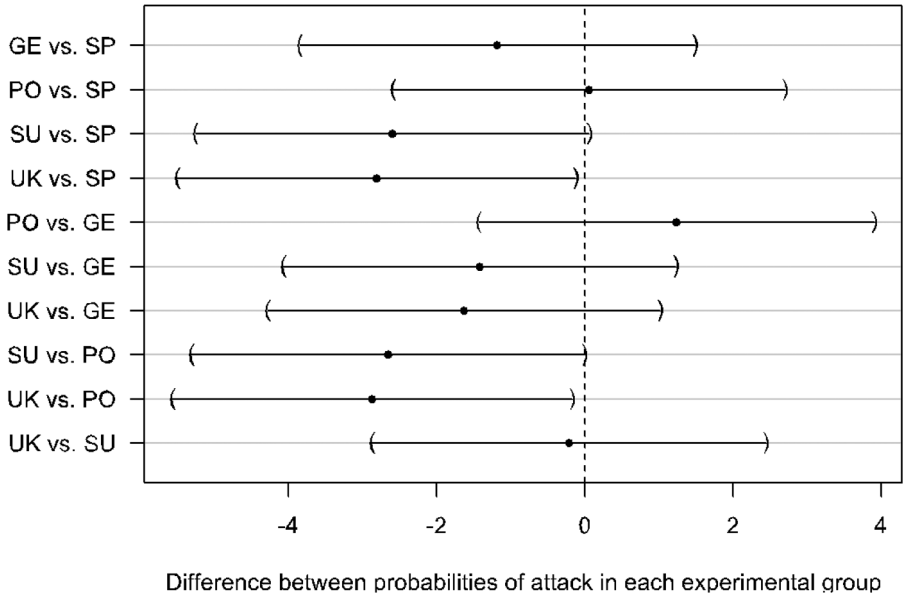

Fig. 4. Confidence intervals for the difference of the average probabilities of suffering a cyberattack between each pair of countries of residence (confidence level 95%).

associated models in order to make sense of this study's findings. Firstly, as noted, the literature so far has predominantly focussed on fear appeals and secondly, we should note that the bulk of the literature has focussed upon health interventions (e.g. attempts to promote smoking cessation or improve diet). However, even in this health literature, there has been a growing recognition that fear appeals made *in isolation* are of limited value in securing behavior change. A meta-analysis of the efficacy of fear appeals (Witte and Allen, 2000) concluded that strong fear appeals work *only* when accompanied by equally strong efficacy messages. They recommended that any intervention must ensure that target populations understand how to perform a recommended response.

In a review of over sixty years of fear appeals research in the health domain that includes six meta-analyses, Ruiter et al. (2014) concluded that fear appeals made in isolation can often be counter-productive. In large part, this is because fear appeals produce defensive responding, particularly in those sectors of the population who are most vulnerable. People may engage in risk denial, biased information processing or simply refuse to attend to the fearful messages, because the threat makes them feel uncomfortable and they have no coping mechanism to know how to deal with that threat.

This assertion is interesting and is somewhat supported by the dropout pattern in our own study. We could argue that dropouts following exposure to the warning message could be taken as a measure of defensive responding (i.e. that dropout is, itself, a useful measure in that it represents a genuine defensive reaction to a security threat). In our data, the dropout was highest following the threat appeal. In other words, while the coping message was effective in equipping participants with the know-how to deal with a security threat, the threat appeal may simply have scared them away. We would argue that further work around this issue would be useful to understand the extent to which dropout might be a viable dependent measure in studies such as this.

Our study offers some findings relating to socio-demographic characteristics. With regard to risk attitudes (as measured by the DOSPERT scale), the study finds that people with a greater appetite for risk navigated less securely than those who were more risk-averse. Moreover, a comparison of risk attitudes between dropouts and non-dropouts revealed significant differences, but only among those in the treatment groups. In other words, those participants who were dissuaded to continue in the experiment by the security notifications tended to be more risk averse than those who continued. While these results are not particularly counterintuitive, they do highlight the relevance of risk attitudes in the study of security behavior, and confirms the utility of the DOSPERT scale for these purposes.

With regard to age, we found that older participants navigated more safely. This is a contribution to the debate on the role of age in online behavior. The literature would seem to suggest that, either because of difficulties in processing information, lack of appropriate social networks, or simply lack of interest, older people would navigate less securely (Esposito et al., 2017; Lunn and Lyons, 2010; Monsuwé et al., 2004; Venkatesh and Morris, 2000). Our results, however, show the opposite. No interaction between age and the treatments were found, showing that the effect of the treatments is not affected by the age of the subjects. However we were unable to test whether our age effects reflected e-commerce experience. It may be possible that older adults were less experienced e-commerce users and took greater care as a result.

The analysis of socio-demographics also yields a case of 'the dog that did not bark'. Education is expected to be relevant in studies such as this one. More educated people should be better equipped to handle the decisions inherent to secure online behavior, as they are less apprehensive about handling a computer (Igbaria and Parsuraman, 1989) and are better able to learn when dealing with sophisticated systems (Bower and Hilgard, 1981). However, education showed no effect. The implication for policy is that 'more education' is not necessarily the answer to unsecure behavior. Rather, it is about providing users with the specific knowledge, at the right point in time, needed to carry out a task.

Finally, regarding the effects of country, participants in Poland and Spain behaved less securely than participants in Sweden and the UK. The underlying reasons for this divergence are not clear. However, this finding is fully consistent with international reports of cybersecurity preparedness at the national level and can be seen as a validation of our methodology. For example, a report by CompariTech on EU countries with the lowest and highest malware infection rates showed Sweden and the UK in the top ten (most secure) and Poland at the bottom (least secure).[6] Our findings highlight the way that individual decision-making strategies differ across countries, and suggest the need to adopt a multi-national approach in studies such as this one, especially if the aim is to produce policy options that are generalizable across contexts.

In summary, messages that contain 'coping' information that support the user in taking action against cybersecurity threat are most effective in improving secure behaviors. Threat messages, presented in isolation, are more likely to lead to a defensive or avoidant response (dropout in our study). This pattern is consistent across countries and across different user profiles. There are communication and policy implications arising from this finding. We should recognize that the 'fear' message is the one most typically propagated via the popular media and workplace campaigns. Thus we are told on an almost daily basis that we are under attack, that data has been lost, that ransomware is on the increase, but such information is usually accompanied by bland and often unhelpful 'coping' information exhorting us to 'stay safe online'. Yet we have shown that stronger coping messages are much more likely to bring about secure behavior change - a finding in keeping with survey data on behavioral intentions (Tsai et al., 2016; Jansen and van Schaik, 2017).

We need to focus more attention on the ways that coping messages are promoted and recognise that, as it currently stands, people are rarely given simple, consistent information about how to deal with a cyber-threat and often don't know which source to trust (Shillair and Meng, 2017). This situation is particularly frustrating, given the observation by Shillair et al. (2015, p. 206) that coping interventions would be particularly useful when prior knowledge of protective measures is weak – which is often the case in relation to protective cybersecurity behavior.

In future work, we could explore more carefully the knowledge gap on appropriate behaviors to take and assess the efficacy of different coping messages on those with different levels of cybersecurity literacy. This would demand a more careful application of PMT in order to understand the way that interventions could target self-efficacy and response-efficacy knowledge and beliefs, but it would also give us more information about the ways in which small behavioral nudges might produce larger security effects. We would also wish to look more carefully at dropout rates across a range of cybersecurity experiments as these are often overlooked but could be considered an important metric for understanding threat avoidance.

Declarations of interest

None.

Acknowledgments

We are grateful to Néstor Duch-Brown, Ioannis Maghiros and Patricia Farrer for their help and support. The study was part of the European Commission's project Behavioural Insights on Cybersecurity (JRC/SVQ/2014/J.3/0039/RC-AMI). The views expressed in this article are purely those of the authors and may not in any circumstances

[6] http://www.visualcapitalist.com/countries-least-prepared-cyber-attacks/

be regarded as stating an official position of the European Commission.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ijhcs.2018.11.003.

References

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science 347 (6221), 509–514.

Adams, A., Sasse, M.A., 1999. Users are not the enemy. Commun. ACM 42 (12), 40–46.

Ajzen, I., 1985. From intentions to actions: a theory of planned behaviour. In: Kuhl, J., Beckmann, J. (Eds.), Action control: From cognition to Behavior. Springer, Berlin, pp. 11–39.

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

Bandura, A., 1997. Self-efficacy: The exercise of Control. W.H. Freeman, New York.

Beautement, A., Sasse, M.A., Wonham, M., 2009. The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 Workshop on New Security Paradigms. ACM, pp. 47–58. https://doi.org/10.1145/1595676.1595684.

Blais, A.R., Weber, E.U., 2006. A domain-specific risk-taking (DOSPERT) scale for adult populations. Judgment and Decision Making 1 (1), 33–47.

Boehmer, J., LaRose, R., Rifon, N.J., Alhabash, S., Cotten, S.R., 2015. Determinants of online safety behaviour: toward a strategy for public education. Behav. Inf. Technol. 34 (10), 1022.

Boer, H., Seydel, E.R., 1996. Protection motivation theory. In: Connor, M., Norman, P. (Eds.), Predicting Health Behavior. Open University Press, Buckingham.

Bower, G.H., Hilgard, E.R., 1981. Theories of Learning. Prentice-Hall, Engelwood Cliffs, NJ.

Briggs, P., Jeske, D., Coventry, L., 2017. Behavior change interventions for cybersecurity. In: Little, L., Sillence, E., Joinson, A. (Eds.), Behavior Change Research and Theory. Elsevier, Amsterdam, pp. 115–136.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34 (3), 523–548.

Burns, A.J., Posey, C., Roberts, T.L., Lowry, P.B., 2017. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Comput. Hum. Behav. 68, 190–209.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., Rao, H.R., 2016. Online shopping intention in the context of data breach in online retail stores: an examination of older and younger adults. Decis. Support Syst. 83, 47–56.

Cisco., 2017. Annual cybersecurity report. Retrieved from. http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1 = 001464170.

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. International Conference of Design, User Experience, and Usability. Springer International Publishing, pp. 229–239.

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

Crossler, R.E., Long, J.H., Loraas, T.M., Trinkle, B.S., 2014. Understanding compliance with bring your own device policies utilizing protection motivation theory: bridging the intention-behavior gap. J. Inf. Syst. 28 (1), 209–226.

Egelman, S., Peer, E., 2015a. Scaling the security wall: developing a security behavior intentions scale (SeBIS). In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, pp. 2873–2882.

Egelman, S., Peer, E., 2015b. The myth of the average user: improving privacy and security systems through individualization. In: Proceedings of the 2015 New Security Paradigms Workshop. ACM, pp. 16–28.

Esposito, G., Hernández, P., van Bavel, R., Vila, J., 2017. Nudging to prevent the purchase of incompatible digital products online: an experimental study. PLoS ONE 12 (3), e0173333. https://doi.org/10.1371/journal.pone.0173333.

European Commission, 2016. European Digital Progress Report. Retrieved from. https://ec.europa.eu/digital-single-market/en/news/commission-releases-2016-european-digital-progress-report-unequal-progress-towards-digital.

Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Social Psychol. 30 (2), 407–429.

Gefen, D., Straub, D.W., 2004. Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. Omega 32 (6), 407–424.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. Comput. Secur. 73, 345–358.

Grimes, G.A., Hough, M.G., Signorella, M.L., 2007. E-mail end users and spam: relations of gender and age group to attitudes and actions. Comput. Hum. Behav. 23 (1), 318–332.

Grimes, G.A., Hough, M.G., Mazur, E., Signorella, M.L., 2010. Older adults' knowledge of internet hazards. Educ. Gerontology 36 (3), 173–192.

Hadlington, L., 2018. The “human factor” in cybersecurity: exploring the accidental insider. In: McAlaney, J., Frumkin, L.A., Benson, V. (Eds.), Psychological and Behavioral Examinations in Cyber Security. IGI Global, Hershey, PA, pp. 46–63.

Hanus, B., Wu, Y.A., 2016. Impact of users’ security awareness on desktop security behavior: a protection motivation theory perspective. Inf. Syst. Manage. 33 (1), 2–16.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125.

Herley, C., 2014. More is not the answer. IEEE Secur. Privacy 12 (1), 14–19.

Hernández, B., Jiménez, J., José Martín, M., 2011. Age, gender and income: do they really moderate online shopping behaviour? Online Inf. Rev. 35 (1), 113–133.

Holt, C.A., Laury, S.K., 2002. Risk aversion and incentive effects. Am. Econ. Rev. 92 (5), 1644–1655.

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 (1), 83–95.

Igbaria, M., Parasuraman, S., 1989. A path analytic study of individual characteristics, computer anxiety and attitudes toward microcomputers. J. Manage. 15 (3), 373–388.

Jansen, J., van Schaik, P., 2017. Comparing three models to explain precautionary online behavioural intentions. Inf. Comput. Secur. 25 (2), 165–180.

Jiang, M., Tsai, H.S., Cotten, S.R., Rifon, N.J., LaRose, R., Alhabash, S., 2016. Generational differences in online safety perceptions, knowledge, and practices. Educ. Gerontology 42 (9), 621–634.

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

Kraemer, S., Carayon, P., Clem, J., 2009. Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput. Secur. 28 (7), 509–520.

LaRose, R., Rifon, N.J., Cotten, S.R., Alhabash, S., Jiang, M., Shillair, R., Rikard, R.V., Cunningham, C., 2015. Generational differences in online safety protection motivation. In: Paper presented at the Amsterdam Privacy Conference 2015, October 23-26, 2015. Amsterdam, Netherlands.

Lee, D., LaRose, R., Rifon, N., 2008. Keeping our network safe: a model of online protection behaviour. Behav. Inf. Technol. 27 (5), 445–454.

Lee, Y., 2011. Understanding anti-plagiarism software adoption: an extended protection motivation theory perspective. Decis. Support Syst. 50 (2), 361–369.

Liang, H., Xue, Y., 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. 11 (7), 394.

Lunn, P., Lyons, S., 2010. Behavioural Economics and 'vulnerable consumers': A summary of Evidence. Economic and Social Research Institute, Dublin Retrieved from. https://www.esri.ie/pubs/BKMNEXT180.pdf.

Maddux, J.E., Rogers, R.W., 1983. Protection motivation theory and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Social Psychol. 19, 469–479.

Martin, N., Rice, J., 2013. Spearing high net wealth individuals: the case of online fraud and mature age internet users. Int. J. Inf. Secur. Privacy 7 (1), 1–15.

Mayer, P., Kunz, A., Volkamer, M., 2017. Reliable behavioural factors in the information security context. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM, pp. 9.

Milne, S., Sheeran, P., Orbell, S., 2000. Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. J. Appl. Social Psychol. 30 (1), 106–143.

Monsuwé, T.P., Dellaert, B.G., de Ruyter, K., 2004. What drives consumers to shop online? a literature review. Int. J. Serv. Ind. Manage. 15 (1), 102–121.

National Cyber Security Centre., 2016. Password guidance: simplifying your approach. Retrieved from. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach.

Neuwirth, K., Dunwoody, S., Griffin, R.J., 2000. Protection motivation and risk communication. Risk Anal. 20 (5), 721–734.

Nurse, J.R., Creese, S., Goldsmith, M., Lamberts, K., 2011, September. Guidelines for usable cybersecurity: past and present. In Cyberspace Safety and Security (CSS), 2011 Third International Workshop on (pp. 21–26). IEEE.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., Ebner, N., 2017. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, pp. 6412–6424.

Pew Research Center, 2017. Americans and cybersecurity. http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

Reid, R., Van Niekerk, J., 2016. Decoding audience interpretations of awareness campaign messages. Inf. Comput. Secur. 24 (2), 177–193.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91 (1), 93–114.

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo, J., Petty, R. (Eds.), Social Psychophysiology. Guilford Press, New York.

Ruiter, R.A., Kessels, L.T., Peters, G.J.Y., Kok, G., 2014. Sixty years of fear appeal research: current state of the evidence. Int. J. Psychol. 49 (2), 63–70.

Saridakis, G., Benson, V., Ezingeard, J.N., Tennakoon, H., 2016. Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. Technol. Forecasting Social Change 102, 320–330.

Sheeran, P., Webb, T.L., 2016. The intention–behavior gap. Social Personality Psychol. Compass 10 (9), 503–518.

Sheeran, P., 2002. Intention—behavior relations: a conceptual and empirical review. Eur. Rev. Social Psychol. 12 (1), 1–36.

Shelton, A.K., Skalski, P., 2014. Blinded by the light: illuminating the dark side of social network use through content analysis. Comput. Hum. Behav. 33, 339–348.

Shillair, R., Dutton, W.H., 2016. Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. Retrieved from. http://dx.doi.org/10.2139/ssrn.2756736.

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.

Shillair, R., Meng, J., 2017. Multiple sources for security: seeking online safety information and their influence on coping self-efficacy and protection behavior habits. In: Proceedings of the 50th Hawaii International Conference on System Sciences. IEEE Computer Society Press, pp. 4977–4986. Retrieved from. http://scholarspace.manoa.hawaii.edu/bitstream/10125/41766/1/paper0617.pdf.

Siponen, M., Mahmood, M.A., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inf. Manage. 51 (2), 217–224.

Smith, V.L., 1976. Experimental economics: induced value theory. Am. Econ. Rev. 66 (2), 274–279.

Sniehotta, F.F., Scholz, U., Schwarzer, R., 2005. Bridging the intention–behaviour gap: planning, self-efficacy, and action control in the adoption and maintenance of physical exercise. Psychol. Health 20 (2), 143–160.

Stevens, M., Chisnell, D., Sasse, A., Krol, K., Theofanos, M., Wald, H., 2014. Report: authentication diary study (National Institute for Standards and Technology). NISTIR 7983 Retrieved from. http://dx.doi.org/10.6028/NIST.IR.7983.

Thaler, R., Sunstein, C., 2008. Nudge: Improving Decisions About Health, Wealth, and Happiness. Penguin, London.

Tischer, M., Durumeric, Z., Bursztein, E., Bailey, M., 2017. The danger of USB drives. IEEE Secur. Privacy 15 (2), 62–69.

van Bavel, R., Rodríguez-Priego, N., 2016. Nudging online security behaviour with warning messages: results from an online experiment. JRC Technical Reports, EUR 28197. https://doi.org/10.2791/2476.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: a protection motivation theory perspective. Comput. Secur. 59, 138–150.

Venkatesh, V., Morris, M.G., 2000. Why don't men ever stop to ask for directions? gender, social influence, and their role in technology acceptance and usage behavior. MIS Q. 24 (1), 115–139.

Vishwanath, A., Harrison, B., Ng, Y.J., 2018. Suspicion, cognition, and automaticity model of phishing susceptibility. Commun. Res. 45 (8), 1146–1166.

Waldrop, M.M., 2016. How to hack the hackers: the human side of cybercrime. Nature 533 (7602).

Weber, E.U., Blais, A.R., Betz, N.E., 2002. A domain-specific risk-attitude scale: measuring risk perceptions and risk behaviors. J. Behav. Decis. Making 15 (4), 263–290.

Witte, K., Allen, M., 2000. A meta-analysis of fear appeals: implications for effective public health campaigns. Health Educ. Behav. 27 (5), 591–615.

Woon, I., Tan, G.W., Low, R., 2005. A protection motivation theory approach to home wireless security. In: Proceedings of the International Conference on Information Systems. Las Vegas, NV. pp. 367–380.

Workman, M., Bommer, W.H., Straub, D., 2008. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. 24 (6), 2799–2816.

Youn, S., 2005. Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. J. Broadcast. Electron. Media 49 (1), 86–110.