A Quantitative Field Study of a Persuasive Security Technology in the Wild

John Paul Vargheese[1(✉)], Matthew Collinson[2], and Judith Masthoff[3]

[1] Edinburgh Napier University, Edinburgh, UK
jpvargheese@acm.org
[2] University of Aberdeen, Aberdeen, UK
matthew.collinson@abdn.ac.uk
[3] Utrecht University, Utrecht, The Netherlands
j.f.m.masthoff@uu.nl

Abstract. Persuasive techniques and persuasive technologies have been suggested as a means to improve user cybersecurity behaviour, but there have been few quantitative studies in this area. In this paper, we present a large scale evaluation of persuasive messages designed to encourage University staff to complete security training. Persuasive messages were based on Cialdini's principles of persuasion, randomly assigned, and transmitted by email. The training was real, and the messages sent constituted the real campaign to motivate users during the study period. We observed statistically significant variations, but with mild effect sizes, in participant responses to the persuasive messages. 'Unity' persuasive messages that had increased emphasis on the collaborative role of individual users as part of an organisation-wide team effort towards cybersecurity were more effective compared to 'Authority' messages that had increased emphasis on a mandatory obligation of users imposed by a hierarchical authority. Participant and organisational factors also appear to impact upon participant responses. The study suggests that the use of messages emphasising different principles of persuasion may have different levels of effectiveness in encouraging users to take particular security actions. In particular, it suggests that the use of social capital, in the form of increased emphasis of 'unity', may be more effective than increased emphasis of 'authority'. These findings motivate further studies of how the use of Social capital may be beneficial for encouraging individuals to adopt similar positive security behaviours.

Keywords: Cybersecurity · Behaviour change · Persuasive technology · Actual effectiveness · Quantitative field study

F. Hopfgartner et al. (Eds.): SocInfo 2022, LNCS 13618, pp. 211–232, 2022.
https://doi.org/10.1007/978-3-031-19097-1_13

1 Introduction

Organisations are increasingly at risk to cyberattacks designed to manipulate users' behaviour to create and exploit cybersecurity vulnerabilities [4,17,101]. This often involves attackers imitating legitimate channels of communications to prompt and trigger insecure behaviour amongst users that can result in their and or an entire organisation's security being compromised [6,28,44,45,68,81]. To address the increasing risk posed by cyberthreats, many organisations invest in and apply technical solutions such as firewalls, anti-virus software, and other tools for monitoring IT systems to maintain security [34,43,53,70,74,86,98]. Despite these efforts, recent studies have emphasised that technical approaches alone are not sufficient [49,50,54,78,96] and organisations continue to be susceptible to cyberattacks [52,71]. This has led to increasing calls for organisations to address individual and organisational factors to maintain their security [74,102]. To achieve this, organisations design security policies to manage users' behaviour and encourage safe and secure usage of their IT systems [16,34,51,59,74,86,87,98]. However, this approach is also insufficient as users' do not always comply with security policies [47,52,62,74,85,87–89,96]. Furthermore, studies investigating causes of insecure behaviour indicate that these are not always related to users' non-compliance with security policies but often overlap with other individual personal and organisational factors [8,13,29,36]. Consequently, users' behaviour continues to be frequently reported as a significant cause of security breaches [26] and there is an increasing need for organisations to discover effective ways to encourage safe and secure behaviour amongst users [12,13,63].

The user's environment, including technological environment and social environment, is composed by factors that influence their behaviour. This suggests the need to bring insights from psychology, including social psychology, to the problem in order to design behaviour change interventions that will address user security behaviours [32,33]. At the same time, technology offers a potential mode for delivering behavioural interventions. If an intervention can be automated, this can allow it to scale-up to larger user bases where other types of intervention may be infeasible. Further, it may be that the most appropriate way to intervene is via technology, for example at the moment that the user's vulnerability is being exploited, or by changing the technological environment. Existing security technologies and management strategies already take advantage of these two benefits of technology, but, perhaps, not always in an optimal fashion.

The field of *persuasive technology* (or the roughly synonymous term *digital behaviour intervention*) is concerned with the study and introduction of technologies that change behaviour, specifically without coercion, with applications across a number of areas. A number of authors from the security domain have suggested that persuasive technologies, and persuasive techniques, may have an important role to play in security [5,8,22,42,100]. While the underlying technology substrate may sometimes be commonplace (for example email in this study), persuasive technology researchers draw upon insights from psychology

in designing interventions on top of that substrate, and use rigorous scientific methods for analysis and evaluation [25,64,91].

One proposed behaviour change approach, much studied in recent years, includes applying behavioural *nudges*, in which re-design of an individual's decision environment ('choice architecture') guides them to make certain choices rather than others. Often the nudge is in a form such that the individual is not explicitly aware of it. Examples of this approach are the MINDSPACE framework [35], and the SCENE framework [30] tailored for cybersecurity. Applications of nudging to cybersecurity include encouraging safer mobile device usage [9,23,92,94], improving password management [55,77], quantitative access control [69], increasing awareness and improving decision making related to social media disclosures and general privacy concerns [2,99].

An alternative approach involves applying *explicit* persuasive messages. This approach is commonly applied within the persuasive technology domain, and has been demonstrated to be effective for changing individuals behaviour across a range of domains by encouraging healthy eating, increasing physical activity, participating in health and wellbeing activities and sustainable ecological behaviour [48,73]. However, study of the use of explicit persuasive messages, such as those based on Cialdini's well-known principles of persuasion [24], together with measures of actual effectiveness, rather than perceived effectiveness, and particularly in-the-wild, has been limited within the context of encouraging users to engage with information security. An exception is a major study of the effectiveness of the 'social proof' persuasive strategy [33].

In this paper, we present results from a large-scale, quantitative, empirical field study of persuasive messaging for encouraging staff in an organisation (a university) to participate in information security awareness (ISA) training. This study was conducted by incorporating explicit persuasive messages based on random assignment of Cialdini's [24] principles of persuasion within an existing corporate communications infrastructure. Evaluation studies of persuasive messages, widely reported in the persuasive technology literature, often involve the use of *perceived effectiveness* as an outcome measure, based on participant self reporting measures [73]. For this study, we used *actual effectiveness* as an outcome measure based on the direct observable behaviour of participants in response to the persuasive messages applied during the study. This provided us with a more objective measure of the persuasive messages' effectiveness in a real non controlled environment. Our results indicate that there are significant differences in the effectiveness of the persuasive messages used in the study and the role of individual and organisational factors. We also discovered that persuasive messages that included reference to the collaborative role of staff to safeguard the university from potential cyberthreats (aligned with the 'unity' persuasive strategy [24]) were more effective compared to those which emphasised the authority imposed, mandatory requirement for all members of staff to complete their training (aligned with the 'authority' persuasive strategy [24]).

In Sect. 2 of this paper we provide an overview of behaviour change and persuasive techniques, followed by a brief review of behaviour change interven-

tions within a cybersecurity context. In Sect. 3 we describe our methodology, study procedure and present our research question and hypothesis. We present the results of our study in Sect. 4. The limitations of the study are discussed in Sect. 5 and in Sect. 6 we review and discuss key findings and outline our plans for future work.

2 Related Work

Interventions capable of changing individual behaviour are increasingly in demand, because of the impact of the negative consequences that may arise from an individual's actions and decisions. For example, poor diet, lack of exercise and smoking, may result in severe health problems. Similarly, insecure usage of IT systems such as clicking on a link within a phishing email and sharing passwords may compromise security. Behaviour change interventions aim to motivate and encourage individuals towards improving their behaviour, in addition to deterring behaviours that can lead to negative and undesirable consequences [73].

2.1 Behaviour Change and Persuasive Techniques

In broad terms, human behaviour may occur as a result of either automatic, indirect (also referred to as System 1) processing and/or reflective, direct (System 2) processing of cues within the context of a given scenario or environment [19,39,76,90]. Many behaviour change interventions and persuasive technology design frameworks incorporate a model of behaviour that may be used to elicit behavioural determinants or factors that may influence and change an individual's behaviour for a given scenario [41,65,72]. Upon establishing how certain behaviours occur and why, it is possible to begin considering what specific techniques may be applied to bring about a desired outcome. However, it is often difficult for intervention designers to establish a suitable theoretical foundation, that provides a testable hypothesis for how and why a particular behavioural change or persuasive technique may influence and determine an individual's behaviour [7,66]. This is often due to the diversity and interrelated aspect of behavioural determinants that may lead to an intervention's means of achieving the intended outcome [31].

Within the Persuasive Technology domain, a common approach towards designing behaviour change interventions involves applying persuasive messages based on principles of persuasion as defined by Cialdini [24]. Such persuasive messages may be designed to bring about changes in behaviour using either 'System 1' or 'System 2' processing, but in the case of the latter, these are intended to trigger a willing change in beliefs and attitudes that may result in a change of behaviour [20,40,84]. Table 1 lists Cialdini's principles and how these may be applied to develop persuasive messages for behaviour change.

An alternative approach that incorporates both the MINDSPACE [35] framework and Cialdini's [24] principles of persuasion is the Behaviour Change Wheel (BCW) [65]. BCW incorporates the Capability, Opportunity, Behaviour

Table 1. Cialdini's principles of persuasion and how these may be applied within persuasive strategies to change behaviour [24]

Principle of persuasion	Potential strategy approach and impact on behaviour
Reciprocity	We are likely to respond in kind as the receiving party in an exchange out of a sense of obligation to do so
Commitment and Consistency	We aim to be consistent in our actions and decision to avoid complexity arising from inconsistencies in our behaviour
Social proof	Our actions beliefs and behaviours may be strongly influenced by what we observe in others as correct and/or appropriate
Liking	We may be significantly influenced by what is attractive and appealing to us
Authority	We will often accept the beliefs and attitudes of those we consider to be within a position of expertise
Scarcity	We are strongly influenced to avoid loss
Unity	Reference to shared identities we define ourselves as a member of together with others can strongly influence our behaviour

(COM-B) model which is based upon a systematic analysis of 19 frameworks of behaviour change [65]. The COM-B model may be used to perform a "behavioural diagnosis" based upon how the three components of this model interact to form behaviour which also has an effect and impact on these components [67]. BCW may be used to link the findings from this analysis to specific intervention types and policies that support their implementation [65,67]. In the next Section, we discuss examples of behaviour change techniques within the security domain.

2.2 Behaviour Change for Cybersecurity

As discussed by Briggs et al. [15], protection motivation theory (PMT) [79] has been applied to a range of studies [21,60,82] investigating users' behaviour within a cybersecurity context. In summary, PMT suggests that individuals will perform protective actions based on a prior assessment of a potential threat (threat appraisal) and their ability to engage in recommended preventative measures (response efficacy and coping appraisal) [79].

Nudges have been suggested as a suitable approach towards changing users' behaviour by aiding decision making related to application privacy settings, in order to avoid unintended disclosure of personal information [1,2,9,10,30]. Users' are often willing to accept a trade-off for security and privacy settings due to what has been described as "Psychological distortions" driven by heuristics, cognitive and behavioural biases such as hyperbolic discounting, lack of self control and immediate gain; that may lead to insecure behaviours [1,2,29]. Nudges may

be applied to address these issues by taking advantage of how users' may be influenced by such 'System 1' and/or automatic cues, to change their behaviour.

For example, Choe et al. investigated positive and negative framing effects via a visual representation of a mobile application's privacy ratings [23]. Results from this study indicate that this is an effective means for increasing users' understanding of the potential risks of installing privacy-invasive mobile applications and how this may discourage users to do so [23]. Van Brugeen et al. investigated how messages based on incentives, morality and deterrence may be used for encouraging users to lock their smartphones [94]. Results of this study indicate that messages based on morality are most effective over time, while those based on deterrence are more immediately effective [94]. Nudges incorporated within personal firewall warning messages have also been demonstrated to be effective with increasing users' risk perception and understanding of the possible negative consequences of their actions in addition to encouraging safer behaviours after receiving such warnings [75].

Kankane et al. conducted a study investigating the effects of five different messages based on incentive, norm, default, salience and ego nudges that may be used to influence users' password management behaviour [55]. Results indicate that the salience nudge was most effective for reducing participants' perceived level of comfort with accepting an auto-generated password and the default nudge was the least effective.

Nudges have also been demonstrated to be effective for improving users' decision making related to selecting wireless network connections. Nudges investigated included using colour coding, order of presentation and a combination of both nudges, to encourage users to select secure rather than less secure wireless network connections. Results indicate that colour coding was more effective compared to ordering, although the combination of both was the most effective for encouraging users to select secure over less secure networks [92].

2.3 Motivation for Study

To develop effective behaviour change interventions to improve cybersecurity, it is necessary to conduct evaluations studies using direct behavioural measurements (actual effectiveness) that provide evidence of how such interventions may change users' behaviour [38,95]. The study presented in this paper investigates the actual effectiveness of persuasive messages designed to encourage university staff to complete ISA training. For ISA training to be effective, user participation is essential [3] and lack of motivation amongst users' to do so may hinder its overall effectiveness [93].

Understanding of actual effectiveness of behavioural interventions calls for repeated laboratory studies (to get insight into 'efficacy' with significant control over variables under ideal conditions), repeated field studies (to understand 'effectiveness' of interventions where variables are less controlled), and an understanding of the causal mechanisms behind the effectiveness of the intervention (to understand the limits of the transport of results from one field to another)

[18,46]. For our contribution, we conducted one, quite large, field study, focusing on comparisons of a small number of interventions of similar type (explicit persuasive messages) in order to have a reasonable experimental design.

For this study, we had available an existing corporate communications infrastructure, using email, but importantly also access to the underlying organisational structure, for example, the communications team, and sign-off from senior management and the IT department. With the constraints of this real-world context, not all forms and strengths of persuasive message would have been appropriate, or possible, to trial.

3 Methodology

The study was conducted at a university with participants consisting of members of staff only. The university requires staff to complete a range of training courses such as health and safety, equality and diversity and ISA training. The usual procedure for delivering such training involves emailing members of staff a notification that such training is available, required to be completed, and how to access it. Training is usually provided by a web service. Over a period of time, the completion rate for the training is monitored and reminder emails sent to those members of staff who have not yet completed it.

The study procedure for our research followed a similar process, incorporating different types of persuasive messages within notification and reminder emails. We describe each stage of the study procedure in the following sections and an overview of the whole process is presented in Fig. 1.

3.1 Study Procedure

Following current practice at the university, all members of staff received a notification email sent on behalf of a senior member of the management. The email included one of four types of persuasive messages (authority, commitment, reciprocity and unity) which were randomly assigned to participants.

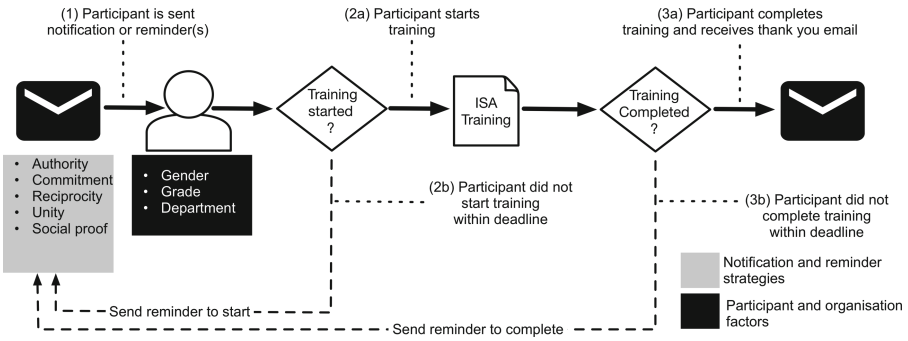

Fig. 1. Study procedure

Two weeks after the original notification emails were sent, reminder emails were sent to members of staff who were yet to start the training. Reminder to start (RTS) emails included a slightly modified and reduced version of the type of persuasive message used in the original notification. This was intended to reduce any possible effect of participants feeling manipulated as discussed in related work concerning repeated use of persuasive messages [97].

Four weeks after the original notification emails were sent, all staff who had not yet completed the training received a reminder to complete (RTC) email. This email was sent irrespective of whether any RTS email had been sent and all RTC emails contained the same Social proof strategy. This strategy aims to influence an individual's behaviour by referring to the behaviour of others in a social context, to encourage an individual to perform the same behaviour [24]. We therefore considered Social proof to be appropriate for RTC emails because this stage of the study provided suitable context for encouraging members of staff to complete the training by referring to those who had already done so.

3.2 Persuasive Messages for Notification and Reminder Emails

Each category of persuasive message used in the study was created using Cialdini's principles of persuasion [24]. We choose not to use scarcity and liking as we believed these would not be suitable for the application context and goal of persuasion (starting and completing ISA training). Each notification email consisted of three sections and was addressed to each member of staff. The first section included one of the following persuasive messages, a generic motivation statement about the training (regardless of which persuasive message participants received) and instructions on how to access the training:

Authority: *The University requires you to complete mandatory Information Security Awareness training. We know that use of our IT systems is crucial to protecting our networks and data.*

Commitment: *You have been issued with a personal IT account. In using this account, you have agreed to usage conditions including compliance with the University's Information Security policy. Following this agreement, please complete Information Security Awareness training.*

Reciprocity: *The University is working hard to protect your personal data and user account against Cyberattacks. To help us with this challenge, we have prepared a short course on Information Security for staff to complete.*

Unity: *All of us can contribute to maintaining the highest standards of Information Security within our University by completing Information Security Awareness Training.*

About the Training: *The University is increasingly at risk to a wide range of threats to Information Security. These include unauthorised access to personal data, disruption to the University network and criminal and fraudulent attacks targeting users. To*

ensure the University is protected against these threats, it is essential that all users are aware of the risks to Information Security and can respond appropriately.

RTS emails consisted of two sections, a slightly reduced and modified persuasive messages of the same category as the prior notification received and access instructions. The RTS strategies are listed as follows:

Authority: *The Information Security Awareness training has been available since the <date-prior-email-received>. All members of staff should complete this training to ensure access to the University's IT Systems is both safe and secure.*

Commitment: *As part of your agreement with the University regarding safe usage of our IT systems, please start your Information Security Awareness training.*

Reciprocity: *We want to ensure that the user account we have provided for you to carry out your duties is both protected and secure. Please start your Information Security Awareness training.*

Unity: *Please start your Information Security and Awareness training and join your fellow colleagues helping to protect and secure our IT Systems.*

Staff members who did not complete the training received the following RTC email, regardless of any category of persuasive message previously received:

Social Proof: *Please join your fellow colleagues by completing your Information Security Awareness training.*

All emails included a standard disclaimer that provided information concerning how data acquired, based on participants' responses to each email received, would be used for research purposes. Further information included details for how participants could have their data removed from our analysis[1]. A link to the research project website was included, that provided more specific details about the research study, with the exception of how different persuasive messages were being used. This was intended as a means to reduce any possibility of priming participant responses, based on revealing the objectives of the research study. Therefore, at the end of the study period, for all participants who did not request for their data to be withdrawn from our analysis, an email was sent stating that further information about the study was available via the research project website, which stated that a range of different persuasive messages has been used in addition to further information about the objectives of the research study. Participants could still withdraw at this stage.

[1] Permission for using opt-out rather than opt-in consent was granted by the university ethics committee, and the emails made it very clear that participation in the study would not impact on work.

3.3 Research Question and Hypothesis

The aim of this study was to gather empirical evidence of the actual effectiveness of persuasive messages for encouraging university staff to complete ISA training. As discussed in Sect. 3, the study procedure followed common practice for encouraging university staff to undertake training courses though the use of notification and reminder emails. This provided a means to investigate the actual effectiveness of the persuasive messages by measuring the distribution of participants' responses throughout the study. Where significant variations in the distribution of participant responses are present, this would suggest that the persuasive messages are not equally effective. This would indicate that at least one persuasive messages was significantly more effective than another. Therefore our research question is as follows:

RQ1 Is the distribution of participant responses the same for all persuasive messages?

To develop a testable hypothesis for RQ1, we categorised participants' responses for those who completed the training as an ordinal dependent variable based on different periods of the study: notification to RTS, RTS to RTC, and RTC to end of study period. A further category for participants who did not complete the training within the study period was also included. This was necessary to ensure the dependent variable was a sufficient measure of actual effectiveness by incorporating all possible participant responses to the persuasive messages during the study. We refer to this measure as *response categories*. Significant variations present in the distribution of response categories would suggest that at least one persuasive message is more effective than another. Therefore our hypothesis for the study is as follows:

H^0 There is no significant variation in the distribution of response categories for all persuasive messages

H^1 There is a significant variation in the distribution of response categories for all persuasive messages

3.4 Confounding Variables

Additional participant data acquired for our analysis included gender, grade[2] and which school of the university participants were associated with. To ensure participants' anonymity was preserved, individual grades of participants were banded into three groups. Grades one to four were grouped into a single band as grade one, grades five to seven were grouped into grade two and all remaining higher grades (eight and nine) grouped into grade three. Grade provides an indication of seniority within the university and also corresponds to participants' age. As such it is possible that participants' grade may have an impact on the distribution of participant responses during the study. We refer to organisational units of the university as 'school' whose disciplines were also anonymised to further ensure participant's anonymity was preserved. As with grade, it is

[2] Grade refers to an ordered grouping of roles within the organisation.

possible that participants' responses may vary based upon which school they are associated with. Although we are required to preserve the anonoymity of Schools, we are interested in discovering whether there are any variations in the distribution of participant responses based on School. Due to this study being run in the wild, we could not ensure equal distribution of persuasive messages based on either participant or organisational factors. Therefore our analysis of the results follows the use of non-parametric statistics as these are suitable in cases where the distribution of the dependent variable is not equally distributed amongst the independent variables [83]. In the next section, we report the main findings of this study and an exploratory analysis investigating whether there are any significant variations in the distribution of response categories and participant and organisational factors(gender, grade and school) is presented in Appendix A.

4 Results

The study was conducted with 1592 participants[3]. The sample included (58%) female, (42%) male, (29%) within grade 1, (52%) within grade 2 and (20%) within grade 3. The distribution of participants across individual Schools is shown in Appendix A, in Table 5, together with results from our exploratory analysis of participant and organisational factors as discussed in Sect. 3.4. We conducted a χ^2 test to discover whether there was a significant imbalance of persuasive messages across participant and organisational factors, for each factor. This is considered suitable to discover whether there is a significant difference in the frequencies of two or more independent groups (persuasive messages, participant and organisational factors) [83]. Results from these tests indicate that there is no significant difference between the frequencies of persuasive messages received based on participants gender ($\chi^2(3) = 5.559, p = .013$), grade ($\chi^2(6) = 12.591, p = .05$) and school ($\chi^2(36) = 32.683, p = .627$).

Table 2 list the distribution of response categories for all persuasive messages. To discover whether there was any significant variation in the distribution of response categories for all persuasive messages, we conducted a Kruskal Wallis test, which is suitable for identifying whether there is a significant difference between two or more groups of an independent variable (persuasive messages) which are not equally distributed using an ordinal dependent variable (response categories) [83]. Results from this test indicate that there is a significant difference in the distribution of response categories for all persuasive messages: ($H(3) = 8.94, p = .03$). These results provide support for H^1 by indicating that there is a significant variation in the distribution of response categories for all persuasive messages. Therefore, we address ***RQ1*** by concluding that the distribution of participant responses is not the same for all persuasive messages. This

[3] This is after the exclusion of staff who opted-out, staff who were excluded as their anonymity could not be guaranteed, and cases where the data showed anomalies such as training being completed before the notifications were sent, e.g. IT staff testing access to the training.

suggests that the persuasive messages are not equally effective and at least one persuasive message is more effective than another.

Following these results, we conducted a post hoc Dunn's test, to discover whether there were any specific significant variations in response categories between the persuasive messages using a Bonferroni correction to control for type 1 errors [37]. We discovered a significant variation in the distribution of response categories between the Unity and Authority persuasive messages ($p = .03, r = .1$). Participants who received the unity persuasive message completed the training earlier, with fewer not completing the training compared to those who received authority. No other significant variation in the distribution of response categories was discovered for any other pairwise comparison of persuasive messages. Therefore, we conclude that the unity persuasive message was more effective compared to the authority persuasive message only. We note that despite a significant variation in the distribution of response categories between the unity and authority persuasive message, the effect size is small [27].

Table 2. Distribution of response categories for each persuasive message

	Persuasive message				
Study period	Authority	Commitment	Reciprocity	Unity	Total
Notification to RTS	164	172	136	157	629
RTS to RTC	86	85	90	86	347
RTC to End	82	71	58	67	278
Not completed	112	85	83	58	338
Total	444	413	367	368	1592

5 Study Limitations

As part of the conditions for ethical approval to perform this study, it was necessary to acquire informed consent by participants using a disclaimer included within the emails sent to participants during the study. Consequently, it is possible that participants may have responded differently if they were not informed about the study in progress. To minimise this effect, participants were only informed that a study on the use of persuasive messages was being conducted but not that different message strategies had been used throughout. This information was later released on the project website and participants who did not opt out of the study, regardless of whether they completed the training or when, received this information as part of the thank you email.

Another condition as part of our ethical approval included the need to mention within the disclaimer, that regardless of whether participants choose to opt out of the study or not, that it was mandatory for members of staff to undertake training as part of university policy. This may also have influenced the participants in addition to type of persuasive message received and as such, each email contained some aspect of the authority principal.

The live nature and environment for this field study limited the way in which the study could be run, and this limits the conclusions that can be drawn. For example, no control or neutral (no persuasive message applied) condition could be applied to participants. This was necessary as part of the conditions for ethical approval to perform the study and to fulfil the university requirement that all members of staff complete the training. It was considered that participants who did not receive a persuasive message containing at least one persuasive principle may be less likely to complete the training compared to those who did receive a persuasive message containing at least one persuasive principle. For a second example, while messages were intended to emphasise one persuasive principle or other, they (through the message itself or source and channel) often contained other factors that could influence behaviour (e.g. other principles). For example, all messages were known to come from an authoritative source (the university). We therefore cannot conclude in all certainty that the effectiveness of a message was a result of its privileged persuasive principle, rather than the result of some other factor.

6 Conclusions and Discussion

This paper presents a study of the relative effectiveness of four persuasive messages for encouraging users to complete ISA training. This study is one of very few which was performed in the wild and measured the actual effectiveness rather than perceived effectiveness of persuasive messages. We observed that there was a significant variation in participants responses to the persuasive messages. This suggests that some persuasive messages differ in effectiveness. There was a significant difference between the responses to the unity and authority persuasive messages, but the effect size associated with the significant variation in participant responses between the two was small. This is perhaps because the different messages had mild variations of emphasis of different persuasive principles, rather than using completely different principles. As discussed in Sect. 3.2, only the first section of each email contained one of the persuasive messages with the remaining content being identical for all emails. Furthermore, as discussed in Sect. 5, each email included some aspect of the authority principle within the disclaimer which may have influenced participants. However, this means that such small changes of emphasis may not make a practical difference.

Our results concerning the unity persuasive message would appear to support claims that individuals may alter their behaviours (within the context of cybersecurity related behaviours) to match others whom they identify as being a part of the same group (in the case of our study, members of staff at the University) [11]. It is possible that the unity persuasive message triggers social capital as the motivation for participants to complete their training, through this message's emphasis on shared collaboration towards a common beneficial goal. As discussed by Sasse et al. [58] individuals within an organisation are, to a certain degree, "emotionally attached" to the organisations they are apart of [61,80] and may be motivated and capable of performing protective behaviours

[14,56,57], which is the overall objective for engaging with ISA training. Herath et al. suggests that motivation to perform security related behaviours (in the case of our study engaging with ISA training) may be influenced by users' "closeness" to organisation they are a part of [50]. At the same time it is possible that the authority message constrains and/or weakens social capital as a motivator by implying that although completing the training is important, this is nevertheless a mandatory (enforced) request. Further studies are required to clarify this.

In future work, we plan to investigate the perceived effectiveness of the persuasive messages using a scenario based approach that provides a greater means to measure specific individual and organisational factors, compared to a field study in the wild. We intend to discover whether the results from such a study would yield similar results with respect to the variations in participant responses to the unity and authority message and to what extent more specific measures of participant and organisational factors may influence participants' susceptibility to the persuasive messages.

Acknowledgements. This research was supported by the UKRI EPSRC award: EP/P011829/1.

A Exploratory Analysis

This section reports results from an exploratory analysis of participant and organisational factors captured during the study. The aim of this analysis was to discover whether there are significant variations in the distribution of response categories for each factor. Our research questions and hypothesis are:

RQ2 Is the distribution of participant responses the same for all participant and organisational factors?

H^0 There is no significant variation in the distribution of response categories for all participant and organisational factors.

H^1 There is a significant variation in the distribution of response categories for all participant and organisational factors.

We expanded ***RQ2*** to ***RQ2a***, ***RQ2b*** and ***RQ2c*** to account for gender, grade and School respectively.

A.1 Analysis of Gender and Participant Responses

Table 3. Distribution of response categories by gender

Study period	Female	Male	Total
Notification to RTS	385	244	629
RTS to RTC	192	155	347
RTC to End	161	117	278
Not completed within study period	181	157	338
Total	919	673	1592

Table 3 shows the distribution of response categories by gender. To discover whether there is a significant variation in the distribution of response categories by participant gender, we conducted a Mann-Whitney U test, which is suitable for identifying whether there is a significant variation in the distribution of an dependent variable (response categories) between two independent groups (male and female). Results from this test indicates that there is an overall significant difference *between female and male* participants ($U(Female = 919, Male = 673) = 328527, twotailed, p = .03, r = .1$). It appears that female participants completing the training earlier with fewer not completing the training compared to male participants. We therefore address ***RQ2a*** by concluding that there was an overall impact of gender on participant responses during the study. We note that despite discovering a significant variation in the distribution of response categories between female and male participants, the effect size is small [27].

A.2 Analysis of Grade and Participant Responses

Table 4 shows the distribution of response categories by participant grade. To discover whether was any significant variation in the distribution of response categories by grade, we conducted a Kruskal Wallis test as discussed in Sect. 4. Results from this test indicate that there is an overall significant variation in the distribution of response categories *between grades* ($H(2) = 10, p = 0.007$). Following these results, we conducted a post-hoc Dunn's test to discover whether there were any specific significant variations in response categories *between grades*. Pairwise comparisons using Bonferroni adjusted p -values reveal a significant difference *between Grades 1 and 3* ($p = .01, r = -.1$) and *between Grades 2 and 3* ($p = .03, r = -.1$). It appears that participants within lower grades completed the training earlier, with fewer participants not completing the training, with the greatest difference being *between Grades 1 and 3* compared to *between Grades 2 and 3*, although we note that effect sizes for these observations are small [27]. We therefore address ***RQ2b*** by concluding that there was an overall impact of grade on participant responses during the study. Results from our

post-hoc analysis suggests participants in lower grades completed the training earlier with fewer participants not completing the training, compared to those in higher grades.

Table 4. Distribution of response categories by grade

Study period	Grade 1	Grade 2	Grade 3	Total
Notification to RTS	198	328	103	629
RTS to RTC	92	188	67	347
RTC to End	73	146	59	278
Not completed within study period	91	165	82	338
Total	454	827	311	1592

A.3 Analysis of School and Participant Responses

Table 5. Distribution of response categories by School

	School													
Study period	1	2	3	4	5	6	7	8	9	10	11	12	13	**Total**
Notification to RTS	191	6	12	94	4	196	34	28	10	9	25	10	10	629
RTS to RTC	100	7	17	48	5	82	24	24	8	8	10	9	5	347
RTC to End	79	4	11	62	6	59	16	10	6	7	12	5	1	278
Not completed within study period	75	9	19	32	12	77	15	23	15	22	19	5	15	338
Total	445	26	59	236	27	414	89	85	39	46	66	29	31	1592

Table 5 shows the distribution of response categories by School. We repeat our approach for analysis grade in our analysis of School using a Kruskal Wallis test. Results indicate a significant variation in the distribution of response categories *between* Schools ($H(12) = 64.1, p < .01$). Table 6 lists all significant pairwise comparisons between Schools, with Bonferroni corrected p values.

For each significant comparison, it appears that participants in Schools 1, 4, 6 and 7 completed the training earlier, with fewer participants not completing the training, compared to Schools 3, 5 and 10, respectively for each comparison listed. Effect sizes for these observations are small. We address ***RQ2c*** by concluding that there was an overall impact of school on participant responses during the study. Due to the needs to preserve the anonymity of schools within the university, our conclusions as to the specific pairwise differences between schools are limited. Further studies are required to investigate what properties of the schools may lead to such results.

Table 6. Post-hoc pairwise comparison of response categories by School with Bonferroni adjusted p values (non significant results have been excluded)

Pairwise comparison		n	z	p	r
School 1	School 5	472	–3.70	.02	–.2
School 6	Schooll 10	460	–4.69	<.001	–.2
School 1	School 10	491	–4.38	<.001	–.2
School 4	School 10	282	–3.91	.01	–.2
School 7	School 10	135	–3.44	.04	–.2
School 1	School 3	504	–3.42	.04	–.2
School 6	School 3	473	–3.76	.01	–.2
School 6	School 5	441	–3.94	.01	–.2

References

1. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of 5th ACM Conference on Electronic Commerce, pp. 21–29 (2004)
2. Acquisti, A.: Nudging privacy: the behavioral economics of personal information. IEEE Secur. Priv. **7**(6), 82–85 (2009)
3. Albrechtsen, E., Hovden, J.: Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. Comput. Secur. **29**(4), 432–445 (2010)
4. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd edn, Wiley, Hoboken (2008)
5. Ashenden, D., Lawrence, D.: Can we sell security like soap?: A new approach to behaviour change. In: Proceedings of 2013 New Security Paradigms Workshop, ACM (2013)
6. Atkins, B., Huang, W.: A study of social engineering in online frauds. Open J. Soc. Sci. **1**(03), 23 (2013)
7. Atkins, L., et al.: A guide to using the theoretical domains framework of behaviour change to investigate implementation problems. Implementation Sci. **12**(1), 77 (2017)
8. Bada, M., Sasse, A., Nurse, J.R.: Cyber security awareness campaigns: why do they fail to change behaviour? In: international conference on Cyber Security for Sustainable Society (2015)
9. Balebako, R., et al.: Nuding users towards privacy on mobile phones. In: Procs of PINC2011: 2nd International Workshop on Persuasion, Influence, Nudge & Coercion through Mobile Devices, vol. 8 (2011)
10. Balebako, R., Marsh, A., Lin, J., Hong, J.I., Cranor, L.F.: The privacy and security behaviors of smartphone app developers. NDSS Symposium (2014)
11. Benson, V., McAlaney, J., Frumkin, L.A.: Emerging threats for the human element and countermeasures in current cyber security landscape. In: Psychological and Behavioral Examinations in Cyber Security, pp. 266–271. IGI Global (2018)
12. Blythe, J.: Cyber security in the workplace: understanding and promoting behaviour change. In: Bottoni, P., Matera, M. (eds.) Proceedings of the CHItaly

2013 Doctoral Consortium co-located with the 10th International Conference of the Italian SIGCHI Chapter (CHItaly 2013), Trento, Italy, 16 September 2013. CEUR Workshop Proceedings, vol. 1065, pp. 92–101. CEUR-WS.org (2013)
13. Blythe, J., Coventry, L., Little, L.: Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In: S.O.U.P.S. 2015, pp. 103–122 (2015)
14. Blythe, J., Koppel, R., Smith, S.W.: Circumvention of security: good users do bad things. IEEE Secur. Priv. **11**(5), 80–83 (2013)
15. Briggs, P., Jeske, D., Coventry, L.: Behavior change interventions for cybersecurity. In: Behavior Change Research and Theory, pp. 115–136. Elsevier (2017)
16. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quart. **34**(3), 523–548 (2010)
17. Button, M., Nicholls, C.M., Kerr, J., Owen, R.: Online frauds: learning from victims why they fall for these scams. Aust. NZ J. Criminol. **47**(3), 391–408 (2014)
18. Cartwright, N.: Evidence-based policy: what's to be done about relevance? Philos. Stud. **143**(1), 127–136 (2009)
19. Chaiken, S., Trope, Y.: Dual-Process theories in Social Psychology. Guilford, New York (1999)
20. Chatterjee, S., Price, A.: Healthy living with persuasive technologies: framework, issues, and challenges. J. Am. Med. Inf. Assoc. **16**(2), 171–178 (2009)
21. Chenoweth, T., Minch, R., Gattiker, T.: Application of protection motivation theory to adoption of protective technologies. In: 2009 42nd Hawaii International Conference on System Sciences, pp. 1–10. IEEE (2009)
22. Chiasson, S., Stobert, E., Forget, A., Biddle, R., Van Oorschot, P.: Persuasive cued click-points: design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE Trans. Dependable Secure Comput. **9**(2), 222–235 (2012)
23. Choe, E.K., Jung, J., Lee, B., Fisher, K.: Nudging people away from privacy-invasive mobile apps through visual framing. In: Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., Winckler, M. (eds.) INTERACT 2013. LNCS, vol. 8119, pp. 74–91. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40477-1_5
24. Cialdini, R.: Pre-Suasion: A Revolutionary way to Influence and Persuade. Simon & Schuster, New York (2016)
25. Ciocarlan, A., Masthoff, J., Oren, N.: Kindness is contagious: study into exploring engagement and adapting persuasive games for wellbeing. In: Proceedings of 26th Conference on U.M.A.P, pp. 311–319. ACM (2018)
26. Coffey, J.W.: Ameliorating sources of human error in cybersecurity: technological and human-centered approaches. In: The 8th International Multi-Conference on Complexity, Informatics and Cybernetics, Pensacola, pp. 85–88 (2017)
27. Cohen, J.: Statistical power analysis. Curr. Dir. Psychol. Sci. **1**(3), 98–101 (1992)
28. Corradini, I.: Building a Cybersecurity Culture in Organizations. SSDC, vol. 284. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-43999-6
29. Coventry, L., Briggs, P., Blythe, J., Tran, M.: Using behavioural insights to improve the public's use of cyber security best practices (2014), uK GOV. Off. for Sci, Ref: GS/14/835
30. Coventry, L., Briggs, P., Jeske, D., van Moorsel, A.: SCENE: a structured means for creating and evaluating behavioral nudges in a cyber security environment.

In: Marcus, A. (ed.) DUXU 2014. LNCS, vol. 8517, pp. 229–239. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07668-3_23
31. Craig, P., Dieppe, P., Macintyre, S., Michie, S., Nazareth, I., Petticrew, M.: Developing and evaluating complex interventions: the new medical research council guidance. Int. J. Nurs. Stud. **50**(5), 587–592 (2013)
32. Das, S., Kim, H., Dabbish, L., Hong, J.: The effect of social influence on security sensitivity. In: S.O.U.P.S. 2014. USENIX Association (2014)
33. Das, S., Kramer, A.D., Dabbish, L.A., Hong, J.I.: Increasing security sensitivity with social proof: a large-scale experimental confirmation. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 739–749. ACM, New York (2014)
34. Dhillon, G., Backhouse, J.: Current directions in is security research: towards socio-organizational perspectives. I.S. J. **11**(2), 127–153 (2001)
35. Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., Vlaev, I.: Influencing behaviour: the mindspace way. J. Econ. Psychol. **33**(1), 264–277 (2012)
36. Douligers, C., Raghimi, O., Lourenco Barros, M., Marinos, L.: Enisa main incidents in the EU. Technical Report, European Union Agency for Cybersecurity (2020)
37. Dunn, O.J.: Multiple comparisons among means. J. Am. Stat. Assoc. **56**(293), 52–64 (1961)
38. ENISA: cybersecurity culture guidelines: behavioural aspects of cybersecurity. Technical Report, European Union Agency for Network and Information Security (2019)
39. Evans, J.S.B.: Dual-processing accounts of reasoning, judgment, and social cognition. Annu. Rev. Psychol. **59**, 255–278 (2008)
40. Fogg, B.: Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufmann, Burlington (2003)
41. Fogg, B.J.: Creating persuasive technologies: an eight-step design process. In: Proceedings of the 4th International Conference on Persuasive Technology, p. 44. ACM (2009)
42. Forget, A., Chiasson, S., Biddle, R.: Persuasion as education for computer security. In: Bastiaens, T., Carliner, S. (eds.) Proceedings of E-Learn 2007-World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, pp. 822–829 (2007)
43. Gallegos-Segovia, P.L., Bravo-Torres, J.F., Larios-Rosillo, V.M., Vintimilla-Tapia, P.E., Yuquilima-Albarado, I.F., Jara-Saltos, J.D.: Social engineering as an attack vector for ransomware. In: 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), pp. 1–6. IEEE (2017)
44. Gordon, S., Ford, R.: On the definition and classification of cybercrime. J. Comput. Virol. **2**(1), 13–20 (2006)
45. Greitzer, F.L., Strozer, J.R., Cohen, S., Moore, A.P., Mundie, D., Cowley, J.: Analysis of unintentional insider threats deriving from social engineering exploits. In: Security and Privacy Workshops (SPW), 2014 IEEE, pp. 236–250. IEEE (2014)
46. Grüne-Yanoff, T.: Why behavioural policy needs mechanistic evidence. Econ. Philos. **32**(3), 463–483 (2016)
47. Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E.: Understanding nonmalicious security violations in the workplace: a composite behavior model. J. Manag. I.S. **28**(2), 203–236 (2011)

48. Hamari, J., Koivisto, J., Pakkanen, T.: Do persuasive technologies persuade? - A review of empirical studies. In: Spagnolli, A., Chittaro, L., Gamberini, L. (eds.) PERSUASIVE 2014. LNCS, vol. 8462, pp. 118–136. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07127-5_11
49. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. **47**(2), 154–165 (2009)
50. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. I.S. **18**(2), 106–125 (2009)
51. Hu, Q., Xu, Z., Dinev, T., Ling, H.: Does deterrence work in reducing information security policy abuse by employees? Comm. ACM **54**(6), 54–60 (2011)
52. Ifinedo, P.: 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 (2012)
53. Ifinedo, P.: Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf. Manage. **51**(1), 69–79 (2014)
54. Jeong, J., Mihelcic, J., Oliver, G., Rudolph, C.: Towards an improved understanding of human factors in cybersecurity. In: 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), pp. 338–345. IEEE (2019)
55. Kankane, S., DiRusso, C., Buckley, C.: Can we nudge users toward better password management?: An initial study. In: Extended Abstracts of the 2018 CHI Conf. on Human Factors in Computing Systems, p. LBW593. ACM (2018)
56. Kirlappos, I., Beautement, A., Sasse, M.A.: "Comply or Die" is dead: long live security-aware principal agents. In: Adams, A.A., Brenner, M., Smith, M. (eds.) FC 2013. LNCS, vol. 7862, pp. 70–82. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41320-9_5
57. Kirlappos, I., Parkin, S., Sasse, M.A.: Learning from "shadow security": why understanding non-compliance provides the basis for effective security. In: Workshop on Usable Security (2014)
58. Kirlappos, I., Sasse, M.A.: Fixing security together: leveraging trust relationships to improve security in organizations. In: Proceedings of the NDSS Symposium 2015. Internet Society (2015)
59. Knapp, K.J., Marshall, T.E., Kelly Rainer, R., Nelson Ford, F.: Information security: management's effect on culture and policy. Inf. Manage. Comput. Secur. **14**(1), 24–36 (2006)
60. LeFebvre, R.: The human element in cyber security: a study on student motivation to act. In: Proceedings of the 2012 Information Security Curriculum Development Conference, pp. 1–8. ACM (2012)
61. Love, L.F., Singh, P.: Workplace branding: leveraging human resources management practices for competitive advantage through "best employer" surveys. J. Bus. Psychol. **26**(2), 175 (2011)
62. Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R., Kumar, M.: Review and insight on the behavioral aspects of cybersecurity. Cybersecurity **3**(1), 1–18 (2020). https://doi.org/10.1186/s42400-020-00050-w
63. Malkin, N., Mathur, A., Harbach, M., Egelman, S.: Personalized security messaging: nudges for compliance with browser warnings. In: 2nd European Workshop on Usable Security. Internet Society (2017)
64. Masthoff, J., Grasso, F., Ham, J.: Preface to the special issue on personalization and behavior change. User Model. User-Adap. Inter. **24**(5), 345–350 (2014). https://doi.org/10.1007/s11257-014-9151-1

65. Michie, S., Atkins, L., West, R.: The Behaviour Change Wheel. A guide to Designing Interventions. 1st ed. Silverback, Great Britain (2014)
66. Michie, S., Johnston, M., Francis, J., Hardeman, W., Eccles, M.: From theory to intervention: mapping theoretically derived behavioural determinants to behaviour change techniques. Appl. Psychol. **57**(4), 660–680 (2008)
67. Michie, S., Van Stralen, M.M., West, R.: The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implementation Sci. **6**(1), 42 (2011)
68. Mitnick, K.D., Simon, W.L.: The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers. Wiley, Hoboken (2009)
69. Morisset, C., Groß, T., van Moorsel, A., Yevseyeva, I.: Nudging for quantitative access control systems. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 340–351. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_30
70. Mouton, F., Leenen, L., Venter, H.S.: Social engineering attack examples, templates and scenarios. Comput. Secur. **59**, 186–209 (2016)
71. Ng, B.Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: a health belief perspective. Decis. Support Syst. **46**(4), 815–825 (2009)
72. Oinas-Kukkonen, H., Harjumaa, M.: Persuasive systems design: key issues, process model and system features. In: Routledge Handbook of Policy Design, pp. 105–123. Routledge (2018)
73. Orji, R., Moffatt, K.: Persuasive technology for health and wellness: state-of-the-art and emerging trends. Health Inf. J. **24**(1), 66–91 (2018)
74. Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards is security policy compliance. In: 40Th Annual Hawaii International Conference on System Sciences, HICSS 2007. pp. 156b–156b. IEEE (2007)
75. Raja, F., Hawkey, K., Hsu, S., Wang, K.L.C., Beznosov, K.: A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In: S.O.U.P.S. 2011, p. 1. ACM (2011)
76. Rangel, A., Camerer, C., Montague, P.R.: A framework for studying the neurobiology of value-based decision making. Nat. Rev. Neurosci. **9**(7), 545 (2008)
77. Renaud, K., Zimmerman, V.: Nudging folks towards stronger password choices: providing certainty is the key. Behav. Public Policy **3**(2), 1–31 (2018)
78. Rhodes, K.: Operations security awareness: the mind has no firewall. Comput. Secur. J. **17**(3), 1–12 (2001)
79. Rogers, R.W., Prentice-Dunn, S.: Protection motivation theory. Handbook of Health Behaviour Research 1 : Personal and Social Determinants, pp. 113–132 (1997)
80. Rousseau, D.M.: Psychological and implied contracts in organizations. Empl. Responsibilities Rights J. **2**(2), 121–139 (1989)
81. Schneier, B.: Secrets & Lies: Digital Security in a Networked World, 1st edn. Wiley, New York (2000)
82. Shillair, R., Cotten, S.R., Tsai, H.Y.S., Alhabash, S., LaRose, R., Rifon, N.J.: Online safety begins with you and me: convincing internet users to protect themselves. Comput. Hum. Behav. **48**, 199–207 (2015)
83. Siegel, S., Castellan, N.J.: Nonparametric Statistics for the Behavioral Sciences, 2nd edn. McGraw-Hill, New York (1988)
84. Simons, H.W., Jones, J.: Persuasion in Society. Taylor & Francis, New York (2011)
85. Siponen, M., Willison, R.: Information security management standards: problems and solutions. Inf. Manage. **46**(5), 267–270 (2009)

86. Siponen, M.T.: Analysis of modern is security development approaches: towards the next generation of social and adaptable ISS methods. Inf. Organ. **15**(4), 339–375 (2005)
87. Son, J.Y.: Out of fear or desire? toward a better understanding of employees' motivation to follow is security policies. Inf. Manage. **48**(7), 296–302 (2011)
88. Spears, J.L., Barki, H.: User participation in information systems security risk management. MIS Quart. **34**, 503–522 (2010)
89. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Comput. Secur. **24**(2), 124–133 (2005)
90. Strack, F., Deutsch, R.: Reflective and impulsive determinants of social behavior. Pers. Soc Psychol. Rev. **8**(3), 220–247 (2004)
91. Josekutty Thomas, R., Masthoff, J., Oren, N.: Adapting healthy eating messages to personality. In: de Vries, P.W., Oinas-Kukkonen, H., Siemons, L., Beerlage-de Jong, N., van Gemert-Pijnen, L. (eds.) PERSUASIVE 2017. LNCS, vol. 10171, pp. 119–132. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-55134-0_10
92. Turland, J., Coventry, L., Jeske, D., Briggs, P., van Moorsel, A.: Nudging towards security: developing an application for wireless network selection for android phones. In: Proceedings of 2015 British HCI Conference, pp. 193–201. ACM (2015)
93. Valentine, J.A.: Enhancing the employee security awareness model. Comput. Fraud Secur. **2006**(6), 17–19 (2006)
94. Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C.R., D'Arcy, J.: Modifying smartphone user locking behavior. In: S.O.U.P.S. 2013, p. 10. ACM (2013)
95. Van Steen, T., Norris, E., Atha, K., Joinson, A.: What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? J. Cybersecurity **6**(1), tyaa019 (2020)
96. Vance, A., Siponen, M., Pahnila, S.: Motivating is security compliance: insights from habit and protection motivation theory. Inf. Manage. **49**(3–4), 190–198 (2012)
97. Vargheese, J.P., Sripada, S., Masthoff, J., Oren, N., Dennis, M.: A dynamic persuasive dialogue model for encouraging social interaction for older adults. In: I.V.A, pp. 464–465. Springer (2013)
98. Villarroel, R., Fernández-Medina, E., Piattini, M.: Secure information systems development-a survey and comparison. Comput. Secur. **24**(4), 308–321 (2005)
99. Wang, Y., Leon, P.G., Scott, K., Chen, X., Acquisti, A., Cranor, L.F.: Privacy nudges for social media: an exploratory Facebook study. In: Proceedings of the 22nd International Conference on World Wide Web, pp. 763–770. ACM (2013)
100. Weirich, D., Sasse, M.A.: Pretty good persuasion: a first step towards effective password security in the real world. In: Proceedings of 2001 Workshop on New Security Paradigms, pp. 137–143 (2001)
101. Williams, E.J., Beardmore, A., Joinson, A.N.: Individual differences in susceptibility to online influence: a theoretical review. Comput. Hum. Beh. **72**, 412–421 (2017)
102. Zimmermann, V., Renaud, K.: Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. Int. J. Hum.-Comput. Stud. **131**, 169–187 (2019)