The Design of Messages to Improve Cybersecurity Incident Reporting

Pam Briggs[1], Debora Jeske[2], and Lynne Coventry[1(✉)]

[1] Northumbria University, Newcastle upon Tyne, UK
{P.briggs,lynne.coventry}@northumbria.ac.uk
[2] University College Cork, Cork, Ireland

Abstract. Cybersecurity suffers from the problem of poor incident reporting. We explored message influences on incident reporting rate. Participants were presented with messages that differed in terms of (i) whether the problem was framed as a technical or a security issue and (ii) the perceived beneficiaries of making a report (benefit to the user, to others vs. no benefit message). Participants were more likely to report a problem if so doing implied some benefit to self, where making the problem more personally relevant might act to reduce social loafing in group settings. They were also more likely to report a technical rather than a security problem and qualitative data suggested that users were sometimes suspicious of messages reporting a security incident – believing that the message itself might be a cybersecurity attack. The findings provide starting points for future research aimed at improving incident reporting.

Keywords: Security · User behavior · Incident reporting · Behavior change · Protection-motivation theory · Social loafing

1 Introduction

Users are generally poor at incident reporting. Research evidence for this comes primarily from studies of technical error reporting, where failure to report is generally seen as problematic both from an organizational, situational awareness perspective [1] but also from an engineering perspective, as such error reports can help in the design of interventions and software improvements [2, 3]. However, failure to report an incident is even more problematic in relation to cybersecurity, where intrusion detection is an important component in cybersecurity defense. The little research that exists reveals that users pay scant attention to warning messages [4] but also shows that passive warnings, i.e. those requiring no user action, are almost universally ignored [5]. There is comparatively little research that shows how incident reporting behavior relates to an organization's security vulnerability – but we do know that the ability to detect and respond to a cybersecurity attack is paramount, just as we recognize that the volume and diversity of attacks are growing exponentially [6].

Security warnings can include notifications about lapsed security certificates or software updates as well as alerts about mobile applications or websites. It is difficult for users to interpret them properly in order to differentiate between real threats, potential threats and false alarms [7]. Well-designed messages can be effective, for

© Springer International Publishing AG 2017
T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 3–13, 2017.
DOI: 10.1007/978-3-319-58460-7_1

example, Egelman et al. [5] found that active warnings helped deter 79% of participants from visiting a potentially harmful website, but overly complex messages are much less effective [8, 9] and can also be misleading [10]. This is particularly problematic for the novice user, who is unclear about the proper meanings of system settings and messages [11]. Given that users are typically under time-pressure to complete other, high-priority tasks, both the intelligibility and the resource demands of messages are important considerations [12] as is over-exposure to a particular message, which can lead to habituation [13].

It is possible to manipulate the design and content of warning messages so as to nudge users into action. Security messages are more effective when the authority of message sender is emphasized [14]; the severity of threat is highlighted [15]; personal risks rather than technical risks are communicated [16, 17] and when the risk to users' private information is highlighted [16]. Messages are also more effective when they are 'active warnings' that require action from the user before progressing, such as swiping over the text to be read [5, 7]. Contextualized, concrete warnings are superior, i.e. those that take the user's current intention into account in order to evoke realistic consequences of action or inaction [14, 18]. We should, however, note that some studies have found no effect of message design. For example, [19] found no difference in the effect of a generic warning compared to one that highlighted specific consequences and [20] showed that altering text and color improved user attention but this was not sufficient to change behavior.

Given these inconsistent findings, it is important to understand more about why people ignore warnings or requests for specific behaviors. Several useful approaches have been adopted here. Firstly, as we have seen, there is the *productive security* approach (e.g. [21]) that sees the decision to ignore messages as a rational choice. Typically, warning messages and requests for action are often unanticipated, potentially disruptive and unquantified in terms of effort required, and while they may be genuine indicators of security threat, they may also be false alarms. Thus, many users prefer to ignore information when they feel the costs of action outweigh the benefits [22] or when they feel that engaging with the new information would disrupt their primary task performance [23]. There will also be individual differences at play here. For example, those with less capacity to respond (e.g. those with low working memory capacity [24] or those experiencing higher task demands [25]) may possess a reduced cybersecurity 'compliance budget' and as a consequence will struggle to make a proactive response.

A second relevant approach is Protection Motivation Theory (PMT) [26], which supposes that users make two important appraisals, a threat appraisal and a coping appraisal. For the first, they assess both the severity of the threat and their own vulnerability to it and for the second, they assess their own understanding and ability to respond as well as the efficacy of making a response. In relation to the first issue of threat appraisal, the average user has a poor understanding of security threats [27] and security incident reporting has been linked to misperceptions of threat and poor cybersecurity beliefs [29, 30]. In relation to the second point, users may be unsure of the appropriate action to take but can also be unconvinced about the efficacy of taking any action. Some evidence for this comes from Workman et al. [30] who observed that perceived response efficacy was one predictor of inaction. This situation is compounded by the fact that many system errors are encountered repeatedly, reducing the sense that a report will be useful or lead to some personal or organizational benefit (see also [31]).

A third approach draws upon the concept of social loafing [32]. That is, in the presence of many other users, an individual user may not react to a request, perhaps assuming that others will make the required response. Certainly, any individual user would not wish to duplicate the input generated by others - a trend particularly prominent in collective work settings [33]. Also, we should note that while users can be persuaded that their own, possibly unique contribution is important [34], social loafing becomes more likely if they believe their own failure to respond goes unnoticed or if they know they cannot be personally identified [35]. Users may be uncomfortable when personally identifiable information is included in problem reports that are sent back to the corporation and shared with others. This, paradoxically, means that inaction can result from either anxiety about being held accountable for the outcome [36–38] or lead to a lack of accountability [33]. Perceived task characteristics may also contribute to social loafing and the underreporting of errors. For example, unattractive tasks often require the use of incentives to encourage employees to report [39]. Also, complex tasks are less likely to lead to personal engagement [37, 40]. If there is no specific information provided regarding the complexity of the reporting task, then users may assume potential complications or excessive work demands [41] which may or may not exist. Thirdly, the efficacy of reporting may be unclear – lack of change or lack of response to user action may reduce motivation to act, thus returning to the earlier point: the perceived redundancy of effort – it will not make a difference.

To a certain extent, reporting can be improved by making users more aware of the personal relevance of an issue or threat [42]. For example, it may be possible to reduce habitual ignoring of system-generated messages by making those messages more personally relevant [7, 11]. The implication is that providing a better rationale for the request may reduce perceptions of response redundancy, i.e. leave people less exposed to social loafing effects. This could be achieved by either personalizing the message or outlining the repercussions of leaving a potential issue unaddressed over time.

This study is a direct response to calls for more research to help us understand how and why individuals may be persuaded to respond to information requests area [1]. The aims were to investigate how the wording of an incident message might influence the reporting of that message and also to explore individual differences in this area. These aims are expressed as three research questions: 1. Are users more likely to report a problem when it is framed as a security or as a technical issue (framing effect)? 2. Can the inclusion of a ‘benefits’ statement (explaining the benefits to either self or others) improve rates of problem reporting? 3. What individual differences might affect users’ problem reporting behaviors?

2 Method

2.1 Study Design

The main focus of this study was an incident reporting task that had been embedded in a distractor task requiring the participants to rate four travel websites.

Distractor Task. The distractor task (and the focus in the participant recruitment message) asked participants to rate four accommodation booking websites:

(1) Booking.com (2) Tripadvisor.com, (3) Bookingbuddy.com and (4) Airbnb.com. Participants were presented with screenshots of the home page for each site.

Incident Reporting Task. After the third booking site screenshot, all participants were presented with a dialogue box that opened with the statement: "*We noted a problem on this page*". This statement was followed by either a security or technical message frame: "*This problem may indicate a security/technical issue*". The second part of the message presented one of three possible benefit conditions. In the benefit-to-self condition, the message stated "*Problem reporting will help us identify the source of the problem and protect you."* In the benefit-to-others condition, the message reported "*Problem reporting will help us identify the source of the problem and protect others in your organization*". In the third (control) condition, no benefit message was presented. Each message ended with the same question: "*Do you want to report the problem?"* The user was required to click on either the "Report" or "Don't report" button to continue. This was thus a 2 (technical vs security framing) * 3 (benefit to self, benefit to others, no benefit statement) factorial design (see Fig. 1 for an example message). Full ethical approval was received from the departmental Ethics Committee.

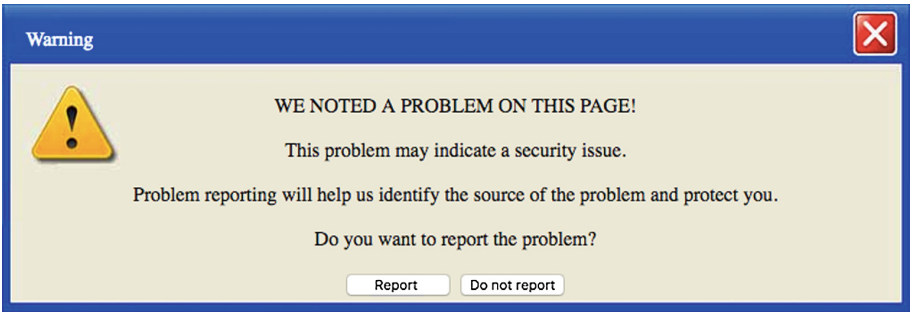

Fig. 1. Example of incident report request message.

2.2 Participants

Participants were university students situated in different departments (social and natural sciences). Information about the study was circulated via email and a dedicated university online recruitment portal. Students are a relevant sample in this case as they tend to use many different online services and had experienced recent server failures. All participants could earn research credits for their respective programs. All participants were recruited between December 2014 and March 2015. In total, the study was accessed by 147 participants. All participants completed the study with a computer and at a location of their choice. Hits that had not led to full completion of the survey were excluded (n = 19). This reduced the final dataset to N = 126. Participants were 18 to 36 years old (M = 20.15, SD = 2.79, n = 125). Eighty-four percent of the participants were female (n = 105, two missing values), only 16% were male (n = 20; one missing value).

2.3 Procedure

Participants were randomly allocated to the six experimental conditions. Once participants had given their consent to participate, they were presented with instructions about how to rate the four online travel sites and each of the four screen shots was then presented separately. Before the fourth screenshot, they encountered a message stating that a problem was found and gave them the choice to report the problem. This was followed by questions about their online use of travel sites, familiarity and review activity of such sites, in turn followed by demographic and short personality questionnaires (no details are included here as no personality effects were found). The questionnaire ended with demographics and the debrief statement about the study.

3 Results

In terms of the message framing, 65 participants received the technical framing, 61 the security framing. In terms of the implied benefit conditions, 41 participants were in the benefit-to-self condition, 37 were in the benefit-to-others condition and 48 participants were in the control condition.

3.1 Incident Reporting Across All Conditions

Overall, 42% of participants ($n = 73$) reported the incident. Table 1 gives a more detailed breakdown and shows, for each condition the number of people who reported the incident with the number who failed to report given in parentheses. The χ^2 statistic revealed a significant overall effect across the six conditions in a 2×3 contingency table ($\chi^2(2) = 8.16$, $p < .05$) but separate analyses for the two experimental manipulations are given below.

Table 1. Number of participants who reported (failed to report) the incident across the six experimental conditions.

	Benefit to self ($n = 41$)	Benefit to other ($n = 37$)	No benefit statement ($n = 48$)
Technical framing ($n = 65$)	24 (0)	6 (11)	5 (19)
Security framing ($n = 61$)	7 (10)	9 (11)	2 (22)

3.2 Effects of Security vs. Technical Framing

There was a significant reporting difference when security vs. technical framing conditions were compared ($\chi^2(1) = 7.65$, $p = .006$). Reporting was higher when the problem was framed as a technical (obs/exp. 35/27.3) rather than a security issue (obs/exp. 18/25.7). The Phi statistic (Phi = −.25) also indicates that there is a moderately strong relationship between framing and reporting. Incident reporting was lower when the problem message suggested a security issue.

3.3 Effects of the Benefit Statement

The χ^2 statistic revealed a significant effect of including a benefit statement ($\chi^2(2) = 33.84$, $p < .001$). Incident reporting was higher when a benefit was implied, particularly a benefit to self (obs/exp. 31/17.2). In the absence of such a statement, reporting was much lower (obs/exp. 7/20.2). The Cramer's V statistic (Cramer's V = .52) also indicates a strong relationship between message contents and reporting responses.

3.4 Qualitative Analysis of General Problem Reporting

Comments were available from 121 of 126 participants. An exploratory analysis was conducted using thematic analysis in order to understand the factors that drove a decision whether or not to report an incident. The quotes provided in this section illustrate the themes that were identified. These themes illustrate the tension between threat perception, the cost of responding and the efficacy of reporting. Non-reporting appeared to be influenced by the extent to which participants sensed a potential threat (fear appraisal), or lack thereof. Some participants actually felt that the message itself represented a threat (as an indicator of a virus or spam). For example, some do not report the problem because: "*I always feel like the message is a virus rather than an actual warning*;" "[*it*] *could be a virus*;" and "*in case it's a scam or a virus*". Others did not perceive a threat and said they felt the message was unimportant or that they had sufficient protection in place and were safe because, for, example "*I have anti-virus software*."

Another factor was the perceived efficacy of responding to the threat with participants reporting that it "*was not worth the effort*" and would make no difference on the grounds of past experience: "*when reporting incidents in the past nothing has happened*". Failure to report may also be linked to uncertainty and lack of information. For example, two participants said that they were "*not sure how it works*" and "*don't know what it means or what it is*". That is, they were unsure of what was required of them or where the information would end up.

A third factor concerned the potential costs associated with incident reporting (e.g., in terms of productivity costs incurred by the process of reporting). Individuals who did not report problems were particularly attentive to the potential time and effort costs associated with making the report. For example, one participant stated that it "*makes it go away quicker if I say no*". In addition, participants reported that "*I just want to continue doing what I was previously and did not want to report an error because of the potential for disruption that may result in terms of "time and redirection*." Lastly there was a suggestion that the request was inappropriate as they had previously been "*taught not to*", suggesting lessons learnt from another part of the security policy (i.e. not clicking on links) was being misapplied in this context.

The participants who accept the error message as legitimate were more likely to go on and report the error. This group recognized the importance of error reporting both for themselves and others, seeking: "*To hopefully draw attention to the problem and ensure it is more likely to be fixed;" "to bring the problem to the attention of the*

website administrator so they can sort it out quicker;" "*to try and stop it from happening from again*;" "*because it may improve future services*;" and "*improve site.*"

4 Discussion

We found that the framing of a message could directly influence incident reporting. Reporting was significantly higher when participants were presented with a technical as opposed to a security framed message, which may relate to concerns participants expressed about security-related messages as a possible social engineering attack. This is a troubling finding when we consider how important security notifications could be in helping us deal effectively with a threat. An additional interpretation (derived from PMT) relates to the user's judgment about whether incident reporting will be effective. Again, users may be more likely to feel that their own organization could respond more swiftly and more effectively in response to a technical problem than to a cybersecurity threat. To a certain extent, people are beginning to habituate to such threats – believing that they must simply accept cybersecurity incidents as part of the working environment. Finally, users may know how to report a technical problem, but be unsure of what action to take in regard to a cybersecurity problem [11].

We also found a significant effect of the benefit message. Reporting frequencies were higher when the message implied a benefit to self, followed by a benefit to others. Reporting was lowest when no benefit information was provided. This was a simple, but effective manipulation and it is interesting to speculate what further information might be used to move users away from social loafing and nudge them into action. Again, in theoretical terms we can see a link to PMT in that a benefit statement explicitly tells users that making a report will produce a positive impact, either to self or other.

4.1 Practical Implications

We deal firstly with the implications that are specific to cybersecurity contexts and here we should note that attempts to nudge action within a security context can backfire. Our manipulations were less effective in the security context and we are particularly concerned about the way that participants felt the message itself could constitute a security threat. We note work by [20] who found that users chose to ignore warnings, believing them to be irrelevant, see [18] who showed that the contextualisation of a message could create distrust and [44] showed that users are often reluctant to use an electronic system to report an incident.

More generally, incident reporting typically represents a situation with unknown "return on investment." Investment here can be understood as the time a user spends on making a report. We would suggest that feedback is important here to boost feelings of efficacy. There should be some acknowledgement that a report has been made and if possibly, some signal of that report's usefulness would be helpful. This point relates to work by [31], who argued that incident reporting will only be perceived as useful when

the data is also used in system improvement and when reporters are made aware that it was their feedback that led to these improvements.

While this study provides interesting evidence about the role of framing in requesting action from a user, we acknowledge that this study was with a group of students using work machines. As such it serves as a proof of concept, and the robustness and transferability of the findings needs to be established as we move forward. An important implication for researchers is to ensure that more work is carried out in this area and that we establish a reliable evidence base about the effectiveness of design interventions within cybersecurity.

4.2 Limitations and Future Steps

Our study provides some important insight into cybersecurity behavior, however, we do acknowledge certain aspects of the study that may be perceived as limitations. In terms of the use of a student sample, it is not unusual for researchers to pilot test interventions with student samples (see examples such as [45–47] or cross-sectional samples that include students (e.g., [7, 48]).

Given the design of the study, it was necessary to carefully monitor of the number of individuals being allocated into each condition. As students are incentivized to complete studies, the drop-out rate was speculated to be lower than with an organizational sample. Choosing students allowed us to anticipate data collection issues (including mid-terms and similar).

However, the use of student samples in the development of potential organizational interventions provide an interesting sample. Students are exposed to cybersecurity messages from their university. They are also unlikely to have had extensive IT training or specific awareness training when joining the university. This provided us with a homogeneous sample than we might get in a more age-diverse organizational setting where individuals may have more expertise (and our effects may be diluted due to less controllable factors). Students will take the behaviors they learn at university into their working life.

This study was a pilot study to test experimental effects for which we lacked a solid foundation, as cybersecurity research has not tackled this issue before. This provides some evidence that these nudges can have a positive effect. However, replication of this study is needed to validate this evidence. The next step would be to implement this approach in organizational settings. This would allow us to ascertain if an effect is still present in a real world setting.

Acknowledgements. We gratefully acknowledge the technical and data collection support of James Turland from the School of Computing at Newcastle University. The work presented in this paper was part of a project (2013–2016) that was funded through the Choice Architecture for Information Security (ChAIse) project (EP/K006568/1) from Engineering and Physical Sciences Research Council (EPSRC), UK, and Government Communications Headquarters (GCHQ), UK, as a part of the Research Institute in Science of Cyber Security.

References

1. Zhao, B., Olivera, F.: Error reporting in organizations. Acad. Manag. Rev. **31**(4), 1012–1030 (2006). http://www.jstor.org/stable/20159263
2. August, T., Niculescu, M.F.: The influence of software process maturity and customer error reporting on software release and pricing. Manag. Sci. **59**, 2702–2726 (2013). doi:10.1287/mnsc.2013.1728
3. Singh, R., Pace, W., Singh, A., Fox, C., Singh, G.: A visual computer interface concept for making error reporting useful at the point of care. In: Henriksen, K., Battles, J.B., Keyes, M. A., et al. (eds.) Advances in Patient Safety: New Directions and Alternative Approaches, Assessment, vol. 1. Agency for Healthcare Research and Quality, Rockville (2008)
4. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: user attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS). ACM, New York (2012). Article No. 3. doi:10.1145/2335356.2335360
5. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1065–1074. ACM, New York (2008). doi:10.1145/1357054.1357219
6. ICS CERT. (2015). https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf
7. Bravo-Lillo, C., Komanduri, S., Cranor, L.F., Reeder, R.W., Sleeper, M., Downs, J., Schechter, S.: Your attention please. Designing security-decision UIs to make genuine risks harder to ignore. In: Proceedings of Symposium on Usable Privacy and Security (SOUPS). ACM, New York (2013). Article 6. doi:10.1145/2501604.2501610
8. Bauer, L., Bravo-Lillo, C.L., Cranor, F., Fragkaki, E.: Warning Design Guidelines. Carnegie Mellon University, Pittsburgh (2013)
9. Harbach, M., Fahl, S., Yakovleva, P., Smith, M.: Sorry, I don't get it: an analysis of warning message texts. In: Adams, A.A., Brenner, M., Smith, M. (eds.) FC 2013. LNCS, vol. 7862, pp. 94–111. Springer, Heidelberg (2013). doi:10.1007/978-3-642-41320-9_7
10. Motiee, S., Hawkey, K., Beznosov, K.: Investigating user account control practices. In: Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems, pp. 4129–4134. ACM (2010)
11. Maxion, R.A., Reeder, R.W.: Improving user-interface dependability through mitigation of human error. Int. J. Hum.-Comput. Stud. **63**, 25–50 (2005). doi:10.1016/j.ijhcs.2005.04.009
12. Böhme, R., Grossklags, J.: The security cost of cheap user interaction. In: Proceedings of the New Security Paradigms Workshop (NSPW 2011). pp. 67–82. ACM, New York (2011). doi:10.1145/2073276.2073284
13. Akhawe, D., Porter Felt, A.: Alice in warning land: a large-scale field study of browser security warning effectiveness. In: Proceedings of the 22nd USENIX Security Symposium, pp. 257–272 (2013). https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_akhawe.pdf
14. Modic, D., Anderson, R.: Reading this may harm your computer: the psychology of malware warnings. Comp. Hum. Behav. **41**, 71–79 (2014). doi:10.1016/j.chb.2014.09.014
15. Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., Cranor, L.F.: Crying wolf: an empirical study of SSL warning effectiveness. In: Proceedings of the USENIX Security Symposium, pp. 399–416. ACM, New York (2009). http://static.usenix.org/legacy/events/sec09/tech/full_papers/sec09_browser.pdf

16. Harbach, M., Hettig, M., Weber, S., Smith, M.: Using personal examples to improve risk communication for security and privacy decisions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2647–2656. ACM, New York (2014). doi:10.1145/2556288.2556978
17. Kauer, M., Pfeiffer, T., Vokamer, M., Theuerling, H., Bruder, R.: It is not about the design - it is about the content! Making warnings more efficient by communicating risks appropriately. In: Proceedings of Conference: Sicherheit– Sicherheit, Schutz und Zuverlässigkeit (2012). http://tuprints.ulb.tu-darmstadt.de/3092/4/ItIsNotAboutTheDesignItIsAboutTheContent.pdf
18. Bartsch, S., Volkamer, M., Theuerling, H., Karayumak, F.: Contextualized web warnings, and how they cause distrust. In: Huth, M., Asokan, N., Čapkun, S., Flechais, I., Coles-Kemp, L. (eds.) Trust 2013. LNCS, vol. 7904, pp. 205–222. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38908-5_16
19. Krol, K., Moroz, M., Sasse, M.A.: Don't work. Can't work? Why it's time to rethink security warnings. In: Proceedings of 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1–10. IEEE (2012). doi:10.1109/CRISIS.2012.6378951
20. Egelman, S., Schechter, S.: The importance of being earnest [in security warnings]. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 52–59. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39884-1_5
21. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the New Security Paradigms Workshop (NSWP 2008), pp. 47–58. ACM, New York (2008). doi:10.1145/1595676.1595684
22. Herley, C.: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: Proceedings of the New Security Paradigms Workshop (NSPW), pp. 133–144. ACM, New York (2009). doi:10.1145/1719030.1719050
23. Duggan, G.B., Johnson, H., Sørli, P.: Interleaving tasks to improve performance: users maximise the marginal rate of return. Int. J. Hum.-Comput. Stud. **71**, 533–550 (2013). doi:10.1016/j.ijhcs.2013.01.001
24. Drews, F.A., Musters, A.: Individual differences in interrupted task performance: one size does not fit all. Int. J. Hum.-Comput. Stud. **79**, 97–105 (2015). doi:10.1016/j.ijhcs.2015.01.003
25. Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: past and present. In: Proceedings of the 5th International Conference on Network and System Security (NSS), pp. 21–26 (2011). doi:10.1109/CSS.2011.6058566
26. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change. J. Psychol. **91**, 93–114 (1975). doi:10.1080/00223980.1975.9915803
27. Furnell, S., Shams, R., Phippen, A.: Who guides the little guy? Exploring security advice and guidance from retailers and ISPs. Comput. Fraud Secur. **12**, 6–10 (2008). doi:10.1016/S1361-3723(08)70175-1
28. Herath, T., Raghav Rao, H.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. **18**, 106–125 (2009). doi:10.1057/ejis.2009.6
29. Howe, A.E., Ray, I., Roberts, M., Urbanska, M., Byrne, Z.: The psychology of security for the home computer user. In: Proceedings of IEEE Symposium on Security and Privacy. IEEE, pp. 209–223 (2012). doi:10.1109/SP.2012.23
30. Workman, M., Bommer, W.H., Straub, D.: Security lapses and the omission of information security measures: a threat model and empirical test. Comput. Hum. Behav. **24**, 2799–2816 (2008). doi:10.1016/j.chb.2008.04.005

31. Holden, R.J., Karsh, B.-T.: A review of medical error reporting system design considerations and a proposed cross-level systems research framework. Hum. Factors **49**, 257–276 (2007). doi:10.1518/001872007X312487
32. Karau, S.J., Williams, K.D.: Social loafing: a meta-analytic review and theoretical integration. J. Pers. Soc. Psychol. **65**, 681–706 (1993). doi:10.1037/0022-3514.65.4.681
33. Karau, S.J., Williams, K.D.: Social loafing: research findings, implications, and future directions. Curr. Dir. Psychol. Sci. **4**, 134–140 (1995). doi:10.1111/1467-8721.ep10772570
34. Kerr, N.L., Bruun, S.E.: Dispensability of member effort and group motivation losses: free-rider effects. J. Pers. Soc. Psychol. **44**, 78–94 (1983). doi:10.1037/0022-3514.44.1.78
35. Harkins, S.G.: Social loafing and social facilitation. J. Exp. Soc. Psychol. **23**, 1–18 (1987). doi:10.1016/0022-1031(87)90022-9
36. Hembree, R.: Correlates, causes, effects, and treatment of test anxiety. Rev. Educ. Res. **58**, 47–77 (1988). doi:10.2307/1170348
37. Jackson, J.M., Williams, K.D.: Social loafing on difficult tasks: working collectively can improve performance. J. Pers. Soc. Psychol. **49**, 937–942 (1985). doi:10.1037/0022-3514.49.4.937
38. Tobias, S.: Test anxiety: interference, defective skills, and cognitive capacity. Educ. Psychol. **20**, 135–142 (1985). doi:10.1207/s15326985ep2003_3
39. Zaccaro, S.J.: Social loafing: the role of task attractiveness. Pers. Soc. Psychol. Bull. **10**, 99–106 (1984). doi:10.1177/0146167284101011
40. Harkins, S.G., Petty, R.E.: Effects of task difficulty and task uniqueness on social loafing. J. Pers. Soc. Psychol. **43**, 1214–1229 (1982). doi:10.1037/0022-3514.43.6.1214
41. Robbins, T.L.: Social loafing on cognitive tasks: an examination of the "sucker effect". J. Bus. Psychol. **9**, 337–342 (1995). doi:10.1007/BF02230973
42. Petty, R.E., Cacioppo, J.T., Goldman, R.: Personal involvement as a determinant of argument-based persuasion. J. Pers. Soc. Psychol. **41**, 847–855 (1981). doi:10.1037/0022-3514.41.5.847
43. Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. **49**, 190–198 (2012). doi:10.1016/j.im.2012.04.002
44. Kingston, M.J., Evans, S.M., Smith, B.J., Berry, J.G.: Attitudes of doctors and nurses towards incident reporting: a qualitative analysis. Med. J. Aust. **181**, 36–39 (2004)
45. Brustoloni, J.C., Villamarin-Salomon, R.: Improving security decisions with polymorphic and audited dialogs. In: Symposium on Usable Privacy and Security (SOUPS) 2007, 18–20 July 2007, Pittsburgh, PA, USA (2007)
46. Gross, R., Acquisti, A.: Information revelation and privacy in online social networks (the Facebook case). In: ACM Workshop on Privacy in the Electronic Society (WPES), 7 November 2005, Alexandria, Virginia, USA (2005)
47. Sun, J., Ahluwalia, P., Koong, K.S.: The more secure the better? A study of information security readiness. Ind. Manag. Data Syst. **111**, 570–588 (2011)
48. Wang,Y., Leon, P.G., Acquisti, A., Faith Cranor, L., Forget, A., Sadeh, N.: A field trial of privacy nudges for Facebook. In: CHI 2014, 26 April–01 May 2014, Toronto, ON, Canada (2014)