Motivating Users to Consider Recommendations on Password Management Strategies

P. Mayer[1,2], A. Kunz[1] and M. Volkamer[1,2]

SECUSO – Security, Usability, Society
[1]Technische Universität Darmstadt
[2]Karlsruher Institut für Technologie

Abstract

It has been proposed to offer users better recommendations on password management strategies. While we support this proposal, we worried whether people would consider and read such recommendations. To that end, we designed a total of nine different messages intended to motivate users to read recommendations on password management strategies and evaluated them in comparison to a control message. To maximise the effectiveness of our messages, we base them on well-established message types and on behavioural factors which have repeatedly been shown to influence human behaviour in the information security context. The most astonishing result for us was that the baseline condition performed as good as the motivational conditions.

Keywords

Motivation, Message Types, Password Management

1 Introduction

Many, usually very stringent, rules regarding secure password usage exist: we should always compose our password as seemingly random strings, change them frequently, never reuse them for multiple purposes, never write them down, never share them with others and the list goes on. The fact is that people face a severe overload (Adams and Sasse, 1999). They can simply not cope with all their passwords. As a result, many users (in particular when not using password managers) decrease the number and/or rigour of the rules they apply (Stobert, 2014). Indeed, often not all rules need to be applied in all contexts in order to render passwords reasonably secure. For more than a decade, security experts have recommended writing down passwords as long as they can be stored securely (Schneier, 2005; Kotadia, 2005). Likewise, password expiration policies have increasingly come under fire (Adams and Sasse, 1999; Chiasson and van Oorschot, 2015; CESG, 2016; Grassi et al., 2017). Some contexts even demand violation of some rules, e.g. when sharing a wifi password with friends or in a family.

Password managers can immensely help decrease a user's mental load associated with passwords, but most users - in particular most lay users - do not use password managers (Hoonakker et al., 2009; Stobert, 2014) and they make false assumptions about the context the password is used for when deciding to decrease the number and/or rigour of the rules they apply (Stobert, 2014). Thus, according to Stobert and Biddle (2015), what is missing are clear recommendations for password management

strategies which include considerations regarding the context (e.g. when applying such coping strategies is viable and when it poses security risks) and the use of password managers. While we concur with this finding, we were afraid that people would not be likely to read such recommendations for the following reasons: (1) because of the abundance of contradicting advice on password security not aligned with current research (Murray et al., 2017), (2) as Beautement et al. (2008) note, users and organisation only have a limited capacity to read and follow new recommendations, and (3) because research has shown that users often do not pay attention to security recommendations or instructions - even when they are right in front of them (Chiasson et al., 2006) and in particular when the material is too involved (Herley, 2009). Also, learning to assess contexts could include a steep learning curve, making motivation essential for an effective learning process (Schiefele, 2009). Thus, we considered it necessary to first motivate people to consider the recommendations.

In this paper, we focus on the motivational step. Our main goal is to develop and evaluate motivating messages regarding their effectiveness. We conducted an online study with nine different motivational messages. Interestingly, and also surprisingly when considering earlier research results (Beautement et al., 2008), our results show that most participants stated a high intention to read our recommendations on password management strategies. Furthermore, our findings support earlier findings that different message types are equally effective (Olembo et al., 2014) and that different behavioural factors are equally effective (private communication with one of the authors of Kajzer et al., 2014).

2 Message Composition

We focus on textual messages to facilitate reuse of our messages in practice: such messages can be easily included in all kinds of information materials (e.g. flyers, newsletters, computer-based trainings, narrated for videos, etc.).

To maximise the effectiveness of our messages, we draw from well-established *message types* described in the literature and *reliable behavioural factors* which have repeatedly been shown to influence human behaviour in the information security context.

2.1 Message Types

Message types represent the general tone of the message. Multiple message types have been proposed and evaluated in different information security contexts (Boss et al., 2015; Siponen, 2014). According to Olembo et al. (2014), only the following message types are relevant in the context of motivational texts:

- *Risk:* Behaviour change is based on communicating risks as well as threats and effective coping strategies.

- *Norm:* Behaviour change is based on communicating how others behave and what social norms exist.

- *Analogy:* Behaviour change is based on exploiting the direct personal experience of the person and drawing parallels between new ideas and existing knowledge.

Due to the lack of empirical evidence regarding the performance of these message types in the area of recommendations on password management strategies, we decided to include all three message types in our study.

2.2 Reliable Behavioural Factors

Additionally, in order to maximise the effect, we phrased our messages so that they would address behavioural factors which have been shown to be reliable predictors of human behaviour in the information security context. Various behavioural theories and corresponding factors have been studied in the information security context. According to Lebek et al. (2014) and Mayer et al. (2017), presenting the results of systematic literature reviews regarding behavioural theories in the information security context, the relevant theories are in particular: Theory of Planned Behaviour, Protection Motivation Theory, General Deterrence Theory, and Technology Acceptance Model. Mayer et al. identify in (Mayer et al., 2017) those factors reliably exhibiting significant results across multiple studies in the information security context. They term the factors fulfilling these criteria *reliable factors*. These reliable behavioural factors are:

- *Perceived Severity of Threats:* magnitude of possible negative consequences, part of Protection Motivation Theory.

- *Response Efficacy:* perceived efficacy of a specific coping action with respect to countering a threat, part of Protection Motivation Theory.

- *Self-efficacy:* the perception of an individual about her/his own ability to successfully perform a specific action, part of Protection Motivation Theory and Theory of Planned Behaviour.

- *Response Cost:* all costs associated with performing a specific coping action, part of Protection Motivation Theory.

- *Attitude:* the feelings of an individual regarding a certain behaviour, part of Theory of Planned Behaviour.

- *Subjective Norms:* any behavioural expectations an individual perceives to be set by her/his environment, part of Theory of Planned Behaviour.

- *Controllability:* an individual's perception of environmental aspects influencing her/his ability to perform a certain behaviour, part of the Perceived Behavioural Control aspect of the Theory of Planned Behaviour.

- *Perceived Certainty of Sanctions:* the likelihood, that an illicit act is followed by sanctions (i.e. punishment), part of General Deterrence Theory.

- *Perceived Severity of Sanctions:* the magnitude of sanctions put on an individual following illicit behaviour of that individual, part of General Deterrence Theory.

- *Perceived Usefulness:* the subjective perceptions regarding increases in productivity stemming from showing a specific behaviour, part of Technology Acceptance Model.

- *Perceived Ease of Use:* an individual's subjective perception of whether using a specific system is free of effort, part of Technology Acceptance Model.

Note that *Subjective Norms* is not considered a factor in the following, since it was already considered as a message type (cf. section 2.1). In addition, two more reliable behavioural factors were excluded from our messages: controllability and attitude. Controllability was excluded since it refers to external aspects (e.g. a website's password policy) which are difficult to control. Attitude was excluded since it refers to an individual's personal feelings. These, by definition, need to be highly personalised to feel appropriate, which is not possible when formulating generic messages as in this work. Each message was designed to address each of the remaining eight behavioural factors.

2.3 Composition of Final Messages

Based on the pre-considerations outlined in the last two sections, we designed for each message type three messages varying the intensity of the phrasing regarding the reliable behavioural factors and one control message (i.e. ten messages in total). The treatment messages were all composed of three parts: (1) an introduction, (2) the motivational part, and (3) a closing sentence leading over to the recommendations. The introduction and the closing part were the same for all the messages, the motivational part was phrased according to the message type (risk, norm, analogy) and the intensity (low, medium, high). The control message was composed only of the introduction and the closing sentence; it did not contain a motivational part. All messages were worded to be used in the context of small and medium-size enterprises (SME). Due to space constraints we can only present two exemplary messages in the following: the control message and one treatment message (risk, low phrasing intensity). The messages are translated to English from their original wording in German.

2.3.1 Control message:

Passwords can fall into wrong hands in a variety of different ways. If we choose weak passwords, they might be guessed easily. If we don't pay attention, we can be observed when entering our passwords. When we write them down, they can be easily stolen.

To prevent such security incidents, plenty of different guidelines exist for securing our passwords: passwords have to be difficult to guess (i.e. as long as possible, and chosen at random), contain numbers and additional characters, contain no information about the user (e.g. date of birth of partner or children), only be used for one purpose (e.g. a user account for PCs, for log-ins on websites, one password for one particular program, etc.), they must not be written down or given away to others and they have to be entered only unobserved. Following all of these rules at all times is difficult. However, a password often doesn't need to fulfil all these rules to be reasonably secure.

The best part of it: Everything you need to know about choosing reasonably secure passwords and remembering them in your everyday life will be explained in the following!

2.3.2 Risk message, low phrasing intensity:

Passwords can fall into wrong hands in a variety of different ways. If we choose weak passwords, they might be guessed easily. If we don't pay attention, we can be observed when entering our passwords. When we write them down, they can be easily stolen.

To prevent such security incidents, plenty of different guidelines exist for securing our passwords: passwords have to be difficult to guess (i.e. as long as possible, and chosen at random), contain numbers and additional characters, contain no information about the user (e.g. date of birth of partner or children), only be used for one purpose (e.g. a user account for PCs, for log-ins on websites, one password for one particular program, etc.), they must not be written down or given away to others and they have to be entered only unobserved. Following all of these rules at all times is difficult. However, a password often doesn't need to fulfil all these rules to be reasonably secure.

The best part of it: It is easy to assess, which rules have to be followed in which situations. Anyone can learn it, even you! This knowledge is useful, because passwords, which are not reasonably secure, are an underestimated risk for competitive medium-sized organisations. Therefore, don’t risk anything! Never be misled to choose passwords, which are not reasonably secure. Everybody, who endangers the organisation, has to expect appropriate consequences. Instead, do your part: Choose reasonably secure passwords to protect the organisation effectively.

Everything you need to know about choosing reasonably secure passwords and remembering them in your everyday life will be explained in the following!

3 Methodology for Empirical Evaluation

To evaluate the effectiveness of our messages, we conducted an online user study. Thereby, we were seeking to answer the following research questions:

RQ_1: Which of the message types (risk, norm, analogy) is most effective regarding motivating potential recipients to read through the recommendations?

RQ_2: Which of the intensity levels of each message type is most effective regarding motivating potential recipients to read through the recommendations?

The study design was developed iteratively in a rigorous process including feedback from experts in the fields of psychology and information security. The final methodology comprises the following four parts:

1. **Brief introduction:** Participants saw a short briefing, explaining the general topic of the study. We did give the participants a scenario of being employed in a SME and having come across the messages in an organisational context. This scenario served to equalise the context in which our messages were interpreted across participants.

2. **Displaying the message:** Then, each participant was randomly assigned to one condition (corresponding to either one of the nine treatment messages or the control message) and the respective message for that condition was shown. Note that, as outlined in section 2.3, our messages included a closing sentence leading over to the recommendations which is necessary for using them in practice. However, the study design did not include any recommendations in order to decrease bias and overhead.

3. **Questions about behavioural intention:** Thereafter, the participant had to indicate her/his intention to read the recommendations on a 5-point Likert scale. The respective item was taken from (Siponen and Vance, 2010) and adopted for our context: *"I intend to read the recommendations on how I can choose reasonably secure passwords for all of my accounts"*.

4. **Demographics:** In the end, the participants had to answer three demographic questions, pertaining to the size of the organisation they work for in their everyday jobs, their profession and their age.

The study was performed using the clickworker crowdsourcing service (an equivalent of the Amazon MTurk service for the German market). The actual survey was realised on a university hosted Limesurey instance. All participants received a compensation of 1.50€ for completing the survey. The methodology of this study conforms to all requirements of our university's ethics commission.

4 Results and Discussion

4.1 Participant Demographics

In total, we collected valid data-sets from 302 participants, where around 30 data-sets could be collected for each of the ten messages. 41.6% of the participants work in small or medium-sized organisations (<500 employees), 20.1% work in large organisations (>=500 employees). The remaining 38.3% chose to not disclose the size of the organisation they work for or are unemployed. Only 15.8% of the participants

work in the IT or IT-security sector. Participants were 18 to 64 years old, the median age being 35 years.

4.2 Effectiveness of the Messages

The overall intention to read the recommendations was high with a mean of 4.13 in the 5-point scale answers. Figure 1 depicts the behavioural intention scores of the ten messages. A closer inspection of our two experimental factors (message type and intensity) with a two-way ATS test (Erceg-Hurn and Mirosevich, 2008) yielded non-significant results on the $\alpha = 0.05$ level for both main effects and the interaction. Consequently, no follow-up tests were conducted.

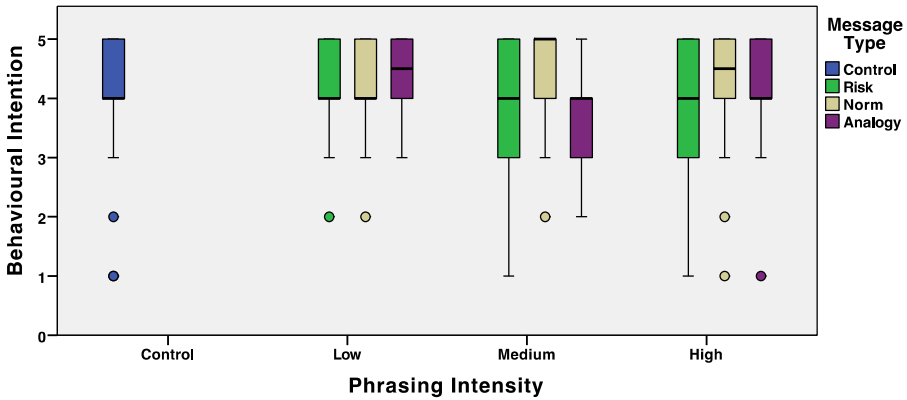

Figure 1: The behavioural intention along the two experimental factors (message type and phrasing intensity)

4.3 Discussion

Our results give further evidence supporting the findings that the different message types are equally effective (Olembo et al., 2014) and that different behavioural factors are equally effective (private communication with one of the authors of Kajzer et al., 2014). The non-significant results of the motivational messages compared to the control group came as a surprise to us. Literature reports significant effects on the behavioural intention for both, the message type (Olembo et al., 2014) and the behavioural factors used in the phrasing of the messages (Mayer et al., 2016). Our results indicate that, although the messages were designed very carefully based on research results, these prior findings cannot be transferred to our scenario of motivating users to read recommendations on password management strategies. We believe that the explanation of these findings lies in the high scores we observed in all conditions, even in the baseline condition (control). A staggering 23 out of 28 participants in the control group stated to either agree or strongly agree in relation to intending to read the recommendations. Therefore, we assume that users are very motivated to read recommendations on how to manage passwords effectively. However, we argue that our results are not only relevant for researchers of password security. They seem to indicate that it is of the essence to assess the baseline

individually for each context and evaluate whether motivational messages are relevant in that specific context. Our results show that in the context of recommendations on password security this does not seem to be the case: the baseline already indicates a high motivation. Yet, in other contexts motivational messages have had success in promoting secure behaviour (e.g. Olembo et al., 2014). Thus, the decision whether motivational messages should be used needs to be investigated for each context individually.

4.4 Limitations

A limitation of our study is that we did not measure actual behaviour, but only behavioural intention. Additionally, we must acknowledge that the scenario we gave the participants restricts our findings to the organisational context. Last but not least, our control message was composed of the introduction and the last sentence which were the same for all treatment messages. While we believe the possibility to be low, a minimal message only stating the existence of recommendations would have allowed us to judge whether the introduction and the last sentence are actually responsible for the motivational effect we observed in all conditions.

5 Conclusion

In this paper, we presented the results of an online user study evaluating the effectiveness of nine different motivational messages. The messages were constructed based on findings in the literature. Interestingly, and also surprisingly when considering earlier research results like (Beautement et al., 2008), our results show that most participants stated a high intention to read our recommendations on password management strategies. Also, our results indicate that (a) different message types are equally effective and (b) that different behavioural factors are equally effective.

6 Acknowledgement

This work has been developed within the project ‘KMU AWARE’ which is funded by the German Federal Ministry for Economic Affairs and Energy under grant no. BMWi-VIA5-090168623-01-1/2015. The authors assume responsibility for the content. This work was further supported by the German Federal Ministry of Education and Research in the Competence Center for Applied Security Technology (KASTEL).

7 References

Adams, A. and Sasse, M. A. (1999), „Users are not the enemy.“, *Communications of the ACM*, Vol. 42, No. 12, pp. 40-46.

Beautement, A., Sasse, M. A., and Wonham, M. (2009), “The compliance budget: managing security behaviour in organisations,” *Proceedings of the 2008 workshop on New security paradigms*, pp. 47–58.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. and Polak, P. (2015), What do users have to fear? "Using fear appeals to engender threats and fear that motivate protective security behaviors.", *MIS Quarterly*, Vol. 39, No. 4, pp. 837–864.

Chiasson, S. and Van Oorschot, P. C. (2015), "Quantifying the security advantage of password expiration policies.", *Designs, Codes and Cryptography*, Vol. 77, No. 2-3, pp. 401-408.

Chiasson, S., van Oorschot, P. C. and Biddle, R. (2006), "A Usability Study and Critique of Two Password Managers." *USENIX Security Symposium*, pp. 1-16.

Communications-Electronics Security Group (2016), "Password Guidance: Simplifying Your Approach." Technical report.

Erceg-Hurn, D. M. and Mirosevich, V. M. (2008), "Modern robust statistical methods: an easy way to maximize the accuracy and power of your research." *American Psychologist*, Vol. 63, No. 7, pp. 591-601.

Herley, C. (2009), "So long, and no thanks for the externalities: the rational rejection of security advice by users." *Proceedings of the 2009 workshop on New security paradigms workshop*, pp. 133-144.

Hoonakker, P., Bornoe, N. and Carayon, P. (2009), "Password authentication from a human factors perspective: Results of a survey among end-users." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 53, No. 6, pp. 459-463.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A. and Van Bruggen, D. (2014), "An exploratory investigation of message-person congruence in information security awareness campaigns." *Computers & security*, Vol. 43, pp. 64-76.

Kotadia, M. (2005), "Microsoft security guru: Jot down your passwords". https://www.cnet.com/news/microsoft-security-guru-jot-down-your-passwords/ [visited: 09.08.2016]

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014), "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, Vol. 37, No. 12, pp. 1049-1092.

Mayer, P., Kunz, A. and Volkamer, M. (2017), "Reliable Behavioural Factors in the Information Security Context." *Proceedings of the 12th International Conference on Availability, Reliability and Security*, No. 9.

Murray, H. and Malone, D. (2017), "Evaluating password advice," *Irish Signals and Systems Conference*.

Grassi, P.A. et al., 2017. Digital Identity Guidelines: Authentication and Lifecycle Management, National Institute of Standards and Technology.

Olembo, M. M., Renaud, K., Bartsch, S. and Volkamer, M. (2014), "Voter, what message will motivate you to verify your vote." *Workshop on Usable Security*.

Schiefele, U. (2009), "Interest and Learning From Text." *Scientific Studies of Reading*, Vol. 3, No. 3, pp. 257–279.

Schneier, B. (2005), "Write Down Your Password", https://www.schneier.com/blog/archives/2005/06/write_down_your.html [visited: 09.08.2016]

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014), "Employees' adherence to information security policies: An exploratory field study." *Information & management*, Vol. 51, No. 2, pp. 217–224.

Siponen, M., & Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations." *MIS quarterly*, pp. 487-502.

Stobert, E. (2014), "The agony of passwords: can we learn from user coping strategies?." *CHI'14 Extended Abstracts on Human Factors in Computing Systems*, pp. 975-980.

Stobert, E. and Biddle, R. (2015), "Expert password management." *International Conference on Passwords*, pp. 3-20.