How to Effectively Communicate Benefits of Introducing a Modern Password Policy to Employees in Companies

Mathieu Christmann*, Peter Mayer◇, Melanie Volkamer◇
* *Technische Universität Darmstadt*
mathieu.christmann@gmail.com
◇ *SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology*
firstname.lastname@kit.edu

Abstract

Traditional password policies comprise rules to enforce a complex composition and demand mandatory changes in frequent intervals. Nowadays, we know that more modern password policies favoring length over complexity and abstaining from frequent password changes offer a better usability and provide higher security compared to the old-fashioned policies. Shifting from such a demanding password policy to a modern one unburdens users long-term and thus, can be used to formulate a deal offering this long-term benefit in exchange for a short-term time cost. In this paper we present a study investigating such a deal: employees of a company were offered to change to a more usable password policy, but in return they were asked to first watch a short explanatory video about password security and then subsequently change their password according to the new policy and the advice in the video. To that end, we created a communication package comprising an introductory email and an explanatory video. The results of our user study show that this approach can be an effective way to shift to a contemporary password policy and – at the same time – raise awareness about issues and misconceptions surrounding password security among users.

1 Introduction

A common response to cyber attacks and insecure human behavior is the implementation of an ever more stringent password policy. Often complex composition rules such as *comp8*[1] are combined with an expiration of the password so that it needs to be changed frequently. Password policies can in general increase security if they are well implemented [10, 21, 22, 24, 27, 31]. However, research shows that users are annoyed by complex password policies and tend to create passwords which meet the requirements, but are easy to guess and as a result not secure [3, 19, 29, 34, 35]. That users have to handle multiple different passwords under such policies is only aggravates these problems. Additionally, many people lack the necessary understanding of password security (e.g., due to misconceptions) [7, 8, 14, 26, 29].

Nowadays, there are modern and less complex password policies (e.g. *basic20*[2]), which provide better security and are more usable [9, 15, 23]. Additionally, it can be questioned if regular password expiration is needed [3, 19] because the goal of this measure, to lock out attackers knowing the password, is not achieved. Also, users develop their own coping strategies. For example, users change their passwords once expired only minimally and write them down on insecurely stored notes [3,19,34,35]. In short, expiration does not only impair security [16, 19, 34, 35], but is also disliked by users [3]. Consequently, governmental standardizing bodies such as *NIST*[3] [17] in the US or the *NCSC*[4] [6] in the UK recommend against expiring passwords on a frequent basis.

Shifting from such a demanding password policy to a modern one that is more usable and also results in strong passwords is possible [23]. Such a shift unburdens the users and can be used to formulate a deal, which is investigated in this work: Users are offered a more usable password policy, but are asked in return to watch a short explanatory video about password security and then change their password according to the advice in the video. Afterwards, the users benefit from better password practices and an easy to handle, long-lasting password, which should also provide higher security [23].

The goal of this work is to investigate if people welcome such a deal and if it can be used to motivate people for awareness measures on password security. To test this approach, a

[1] *comp8* requires at least 8 characters in total, at least one lower letter, one upper letter, one digit, and one symbol

[2] The only requirement of the *basic20* policy is a minimum length of 20 characters with no further requirements.

[3] National Institute of Standards and Technology, USA

[4] National Cyber Security Centre, UK

communication package was created and used to gather initial feedback in a user study with 21 participants. The results showed that the approach can be successfully used to transition a company away from an outdated and tedious password policy requiring users to frequently change passwords and guiding users in this process. At the same time, the approach allows raising awareness about issues and misconceptions surrounding password security among users.

The remainder of this paper is structured as follows. First, we introduce the communication package (i.e., email and video) and its creation procedure (section 2). Then, we present the user study investigating the perceptions of the deal and gathering feedback for improvements (section 3). Finally, we conclude by discussing lines of future work (section 4).

2 Creation of a Communication Package

The prevalent password policies today require rather short but complex passwords [12]. Therefore, the communication package is tailored to companies which currently use such password policies and which also mandate that employees have to change their passwords frequently. This prerequisite is needed to make the deal as described in the introduction[5] viable and to offer an incentive to the employees. Initially accepting the deal is on a voluntarily basis, but the new password policy should apply to every employee eventually. This paper focuses on the initial stage of voluntary transition. The communication package consists of two parts: an email to communicate (i.e. offer) the deal to employees as well as an explanatory video about passwords.

2.1 Requirements

To provide an effective communication package, requirements were drawn from the research literature. These requirements were categorized into two groups: (a) content requirements list important topics, which need to be covered by the explanatory video and (b) design requirements describe how to design the communication package around the content. An overview of all requirements can be found in table 1.

As a basis for the content, we chose the existing awareness-raising material described by Mayer et al. [13, 14] which covers both, attacks and misconceptions. It provided a good basis for this work, since it is publicly available[6] in German (as required by our user study) and its effectiveness was shown in a user study. The material covers five attacks and 14 misconceptions concerning password security that were deemed relevant in the context of our video. These attacks and misconceptions represent the content, which should be explained in the video.

The set of design requirements is based on a literature research. Overall, seven requirements were identified and considered during the creation of the communication package to ensure an effective presentation of the contents.

2.2 Email Offering the Deal

The email was created in an iterative process. It was designed to introduce employees to the new password policy and to motivate them to first watch the video and then subsequently create a strong password. Also, the deal is described and the mail covers several implementation requirements. After reviews of experts[7] as well as laypeople and integration of their suggestions for improvement, the final version was formulated, which can be found in appendix B.

2.3 Explanatory Video

The explanatory video is intended to offer advice to the audience on password security and raise awareness by covering the attacks and misconceptions listed in the requirements. Furthermore, all design requirements should be adhered to during the creation of the video.

As first step in the creation of the video, a story book was outlined. This story book described the scenes, actions, and dialogues of the video. References to the requirements ensured that all requirements would be fulfilled. The story for the video takes place in an office, to capture the business context in which the video is to be used. One of the protagonists is an employee called Bob, who starts his workday. While logging into his computer, he is notified that his password has expired. Bob is annoyed by the message and changes his password only minimally[8], which is a usual behavior according to research. Later, Bob receives an email of the IT department offering Bob the deal. Bob is quite interested in the changes but also has some questions. When Alice, an employee of the IT department, comes by, Alice and Bob have a conversation about the new password policy. In this conversation the bulk of the content, i.e., the attacks as well as misconceptions, are explained based on the design requirements.

Subsequently, the story book was reviewed by experts and laypeople. From the feedback provided by the experts and laypeople, improvements were derived and the final version of the story book was created. Based on this final story book, the explanatory video was created as an animated video using the animation tool *Powtoon*[9]. *Powtoon* offers pre-defined character sets, scenes, and a variety of animations for characters (e.g. speaking or walking). The dialogues were generated using *Microsoft Speech Studio*[10], which offers a powerful text-to-speech service with neural voices. The final explanatory video can be accessed online[11].

[5] Offering a more usable password policy and in return asking to watch the explanatory video and afterwards to create a new and strong password.

[6] https://secuso.aifb.kit.edu/downloads/Schulungen/Modul_Passwortsicherheit.pdf

[7] The mail was presented and discussed, e.g. regarding comprehensibility, motivating word choice and length.

[8] from "Sunshine!3" to "Sunshine!4"

[9] https://www.powtoon.com/

[10] https://azure.microsoft.com/de-de/services/cognitive-services/text-to-speech/

[11] https://www.dropbox.com/s/lhvuh6n94dv9zyb/2021-05-26-WAY-Final.mp4?dl=0

3 User Study

To gather some first feedback on this approach, a small online user study was conducted with employees from a company. The user study was not intended to be representative but to only provide first insights on the effectiveness and potential of the communication package.

3.1 Procedure

The user study was implemented in *SoSciSurvey*[12] platform and consisted of the following phases:

Introduction and Informed Consent. All participants started with a short introduction about the study. They received information regarding privacy and had to provide a consent for participation. Furthermore, basic demographic data (e.g. age group) has been requested.

Sentiment towards Expiring Passwords. Participants were asked about their emotions regarding the need to change their passwords on a regular basis.

Introduction to the Study Scenario. Next, participants were introduced to the study scenario. They were told to imagine that all communication in the remainder of the study really came from their IT department.

Introductory Mail. Then, the participating employees received the introductory mail and were asked what they would do after reading the email.

Explanatory Video. Thereafter, the explanatory video was shown to them and they were asked if they would take on the offer and change to the new password policy and if they would implement the advice explained in the video to create their new password.

Deal. Participants were asked if they have identified a deal in the mailing or the video. If not, the deal was explained to them. Then, the sentiment regarding the deal was inquired. Further questions regarding improvements of the deal were presented.

Further Suggestions. To collect further feedback concerning the email and the video, several questions regarding length as well as positive and negative aspects of the video and email were included.

All questions of the survey can be found in appendix C. Open questions were categorized using inductive coding [4, 28] to derive quantitative statements. The coding was reviewed by two researchers to ensure objectivity and prevent deviations due to personal interpretation.

3.2 Participants

As outlined in section 2, the communication package is geared towards companies currently using a traditional and complex password policy including expiring passwords. Therefore, we recruited participants from a company that currently has such a password policy in place. The reason of this company for still using *comp8* is that its network consists of multiple companies across the world, which need to maintain a common password policy, which is accepted by each company and implementable for all IT systems. In total 24 participants from this company could be recruited into our study. Three participants had to be excluded due to incomplete responses. For another four participants the data showed that they did not watch the video completely. Since their answers pertaining to other aspects than the video were sensible they were, however, not fully excluded from the analysis.

Two thirds of the 21 participants are female and one third is male. Most participants (62%) belong to the age group 21-29, 19% are between 30 and 39. 10% each belong to age groups 40-49 and 50-59.

[12] https://www.soscisurvey.de/

3.3 Results

3.3.1 Expiring Passwords

12 participants (57%) expressed negative emotions, when talking about expiring passwords. They often felt annoyed (33%) or stressed (19%). One participant disliked expiring passwords simply because he is not allowed to use any of the previous ten passwords but would be fine with it otherwise: “Really exhausting if the range is so narrow that I cannot use one of the last 10 passwords. I am fine with the requirements above.” Six participants (29%) have a neutral opinion about expiration. Of those, one participant is unsure if “changing the strong password every 90 days is actually necessary”. Another participant is "fine" with the expiration. 33% of participants think that expiring passwords are necessary for high security, which is a misconception [19].

3.3.2 Email Offering the Deal

17 participants (81%) state that they would watch the video after reading the email, whereas two participants (10%) would just change their password according to the new policy without watching the explanatory video. After receiving the email but before watching the video, one participant is not satisfied with the new password policy and intends to "submit a complaint telling the IT security department that the previous password policy was better". In this case the mailing has not been effective enough to convince the participant of the new password policy. Another participant has a similar sentiment: he is willing to watch the explanatory video, but also wants to "check if the new requirements are strong enough for our needs", which shows the security awareness of the participant and his skepticism.

Most participants (90%) find the length of the email appropriate, while two participants (10%) rate it as too long.

3.3.3 Explanatory Video

16 participants (76%) stated that they intended to completely follow the recommendations described in the video, whereas five participants (24%) would partially follow. There is no

participant that would not follow the recommendations mentioned in the video at all.

Regarding the open question of the user study how participants would implement the recommendations of the video, 17 participants (81%) repeat in their own words how to generate a secure passphrase, which shows that the idea of passphrases is accepted by the participants and the most important points to consider[13] are understood. Interestingly, six participants (29%) report that they would still add numbers and special characters to achieve higher security, even though this is not obligatory but still allowed according to the explanatory video. Presumably, these participants feel safer when using additional character classes.

The way how the learning points are explained in the video is considered as good by 18 participants (90%) and as partially good by 2 participants (10%). 11 participants (55%) state that the duration of the video is appropriate, while nine participants (45%) would prefer a shortened version.

3.3.4 Deal

Using the email and the video together as communication package, a deal was formulated and offered to the participants. After watching the video, 100% of the participants stated that they would comply with the request to change their password afterwards (even the one participant who had previously stated to protest the change). This shows that the purpose of the communication package is fully achieved, although only 16 participants (76%) have identified a deal or an offering within the communication package. Anyhow, even the participants who have not identified a deal, seem to follow the appeal to comply and change the password according to the new policy. This could, however, also be due to the organizational setting and the study scenario in which their IT department issues the communication. Therefore, participants might simply follow the instructions as is common in their company.

After explaining the deal explicitly to the participants, who had not identified it previously, 16 participants (84%) like the deal and two participants (11%) are neutral to the deal.

Three participants are very surprised that non-expiring passwords can offer sufficient security, which indicates a prevalence of the respective misconception among the participants. Also, some participants call the deal very fair after comparing the time for watching the video versus the time needed for renewing their passwords. Evaluating costs against benefits corresponds to findings in current research [7, 20].

3.4 Discussion

The communication package consisting of the email – which gives an introduction to the campaign – and the explanatory video – which offers advice to the employees regarding password security as well as the new password policy – seems to be a promising approach to advertise a shift to a modern password policy in the form of a deal. Although not all participants identified the deal, all were willing to change the password according to the advice after reading the mailing and watching the educational video. Additionally, four participants reported that they highly welcome education on passwords and are happy to learn new things about this topic. Nevertheless, this approach may not be the only successful way changing to a new password policy[14]. Furthermore, the results are potentially impacted by social desirability bias and self-report limitations [18].

Beside the positive feedback, the participants' responses in the user study provided further insights on how to improve the communication package, e.g., making it interactive. Also, participants voiced the wish to receive a one-pager containing the most important learning points. We plan to address both of these issues in future work.

4 Future Work

We created a communication package consisting of an introductory mailing and an explanatory video covering five attacks and 14 misconceptions about password security as well as seven implementation requirements. The communication package can be used by companies, which plan to shift from an old-fashioned to a modern password policy, to educate their employees on password security, and to motivate them to choose more secure passwords for their work accounts.

The communication package was well received, indicating that the overall approach is sound. However, several aspects that need improvements could be identified. In particular the wish to make the video interactive was unexpected, as this would potentially increase the time needed to properly interact with it and the length of the video was already perceived as too long by some participants. Yet, creating an interactive version of the video might allow users to, e.g., have their new passwords checked against a blacklist. A comparative evaluation of an improved video and an interactive version seems to be indicated as future work.

Other lines of future work include enhancing the email or further clarify the deal to the audience, as this core aspect was not fully grasped by all participants. Implementing these suggestions could potentially lead to even better results and an increased effectiveness. A representative and more extensive user study needs to be performed, which also covers further research questions. It should be examined which attacks and misconceptions are well mediated and which must be improved. Also, the effects of the communication package on password security have not been examined. Therefore, it is unknown if the new password and behavior of the participants are indeed more secure than before. Additionally, it should be checked if participants indeed change their password or just state to do it. Future studies will aim to address these short-comings.

[13] e.g. not using personal information

[14] There was no previous communication for the reasoning behind the choice of the password policy in the company.

Acknowledgments

This research was partially supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS).

References

[1] Anne Adams and Angela Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, 12 1999.

[2] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour?, 2019.

[3] Ingolf Becker, Simon Parkin, and M. Angela Sasse. The rewards and costs of stronger passwords in a university: Linking password lifetime to strength. *USENIX Security Symposium*, pages 239–253, 2018.

[4] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3:77–101, 01 2006.

[5] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 Ways to Nudge: A review of technology-mediated nudging in human-computer interaction. In *Conference on Human Factors in Computing Systems*, 2019.

[6] National Cyber Security Center. The problems with forcing regular password expiry. `https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry`.

[7] Cormac Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. *New Security Paradigms Workshop*, pages 133–144, 2009.

[8] Jeffrey L. Jenkins, Alexandra Durcikova, Grayson Ross, and Jay F. Nunamaker. Encouraging users to behave securely: Examining the influence of technical, managerial, and educational controls on users' secure behavior. *International Conference on Information Systems*, 2010.

[9] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of Passwords and People: Measuring the Effect of Password-Composition Policies. *Conference on Human factors in computing systems*, page 2595, 2011.

[10] Cynthia Kuo, Sasha Romanosky, and Lorrie Faith Cranor. Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security*, pages 67–78, 2006.

[11] C. Lin and A.S. Kunnathur. Toward developing a theory of end user information security competence. *Americas Conference on Information Systems*, 5:3578–3587, 01 2013.

[12] Peter Mayer, Jan Kirchner, and Melanie Volkamer. A second look at password composition policies in the wild: Comparing samples from 2010 and 2016. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 13–28. USENIX, 2017.

[13] Peter Mayer, Christian Schwartz, and Melanie Volkamer. On the systematic development and evaluation of password security awareness-raising materials. In *Annual Computer Security Applications Conference*, pages 733–748. ACM, 2018.

[14] Peter Mayer and Melanie Volkamer. Addressing misconceptions about password security effectively. In *International Workshop on Socio-Technical Aspects in Security and Trust*, pages 16–27. ACM, 2017.

[15] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring password guessability for an entire university. *ACM Conference on Computer and Communications Security*, pages 173–186, 2013.

[16] Hazel Murray and David Malone. Evaluating password advice. *Irish Signals and Systems Conference*, 2017.

[17] National Institute of Standards and Technology. Nist special publication 800-63b, 06 2017. `https://pages.nist.gov/800-63-3/sp800-63b.html`.

[18] Elissa M. Redmiles, Y. Acar, Sascha Fahl, and Michelle L. Mazurek. A summary of survey methodology best practices for security and privacy researchers. Technical report, 2017.

[19] Karen Renaud and Verena Zimmermann. Guidelines for ethical nudging in password authentication. *SAIEE Africa Research Journal*, 2018.

[20] Karen Renaud and Verena Zimmermann. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy*, 2019.

[21] Richard Shay and Elisa Bertino. A comprehensive simulation tool for the analysis of password policies. *International Journal of Information Security*, 8:275–289, 08 2009.

[22] Richard Shay, Abhilasha Bhargav-Spantzel, and Elisa Bertino. Password policy simulation and analysis. pages 1–10, 01 2007.

[23] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security*, 18(4), 2016.

[24] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the sixth symposium on usable privacy and security*, pages 1–20, 2010.

[25] Stefan Stieglitz, Tobias Potthoff, and Tobias Kißmer. Digital Nudging am Arbeitsplatz. *HMD Praxis der Wirtschaftsinformatik*, 2017.

[26] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Trans. Priv. Secur.*, 21(3), April 2018.

[27] Wayne Summers and Edward Bosworth. Password policy: The good, the bad, and the ugly. In *Proceedings of the winter international synposium on Information and communication technologies*, pages 1–6, 01 2004.

[28] David R. Thomas. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2):237–246, January 2006.

[29] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "i added '!' at the end to make it secure": Observing password creation in the lab. In *Symposium On Usable Privacy and Security*, pages 123–140, Ottawa, July 2015. USENIX Association.

[30] Melanie Volkamer and Benjamin Bachmann. Wie sie ihre mitarbeiter für it-sicherheit sensibilisieren. `https://www.verwaltung-der-zukunft.org/oeffentliche-it/wie-sie-ihre-mitarbeiter-fuer-it-sicherheit-sensibilisieren`.

[31] Kim-Phuong Vu, Robert Proctor, Abhilasha Bhargav-Spantzel, Bik-Lam Tai, Joshua Cook, and E. Schultz. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65:744–757, 08 2007.

[32] M. Yıldırım and I. Mackie. Encouraging users to improve password security and memorability. *International Journal of Information Security*, 2019.

[33] Nur Haryani Zakaria. Exploring human factors issues & possible countermeasures in password authentication. 2013.

[34] Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. *ACM Conference on Computer and Communications Security*, pages 176–186, 2010.

[35] Leah Zhang-Kennedy, Sonia Chiasson, and P Oorschot. Revisiting password rules: Facilitating human management of passwords. In *APWG symposium on electronic crime research*, pages 1–10, 06 2016.

A Requirements Overview

Table 1: Overview of requirements covering both, content and design requirements.

Category	ID	Source	Description
Content Requirements			
General	G.1	M1 [13, 14]	Attackers are not only criminal hackers but also people you know.
General	G.2	M2 [13, 14]	People believe that they are not important enough to be targeted by an attacker.
General	G.3	M3 [13, 14]	Security requirements do not depend on how often the service is used.
General	G.4	M4 [13, 14]	Security is not only the responsibility of the IT department.
Creation	C.1	A7 [13, 14]	Targeted guessing
Creation	C.2	A8 [13, 14]	Unspecified guessing
Creation	C.3	M12 [13, 14]	The attacker can automate attack A8.
Creation	C.4	M13 [13, 14]	Keystrokes are not secure passwords (even if they contain special characters and numbers).
Creation	C.5	M14 [13, 14]	Attackers adapt the word lists to the attack targets.
Creation	C.6	M16 [13, 14]	Passwords are not automatically more secure by special characters as well as numbers and must be as long as possible.
Creation	C.7	M17 [13, 14]	Software automatically concatenates single entries of the word list and mimics human behavior.
Creation	C.8	M18 [13, 14]	Birth dates do not make passwords more secure either.
Creation	C.9	M20 [13, 14]	Prefer a long password of letters to a short password of all character categories.
Management	M.1	A2 [13, 14]	Stealing an insecurely stored note
Management	M.2	M6 [13, 14]	Write down passwords in the beginning until you know them by heart instead of reusing passwords.
Management	M.3	M19 [13, 14]	Changing passwords as a precaution does not increase security. The password should only be changed in case of an incident.
Management	M.4	M21 [13, 14]	Even strong passwords should not be reused.
Management	M.5	A10 [13, 14]	Stealing unencrypted electronic notes
Entering	E.1	A3 [13, 14]	Shoulder surfing
Design Requirements			
Design	I.1	[13,14,29,33]	Identify risks and consequences, then describe the solution.
Design	I.2	[1, 2, 7, 11, 13, 14, 25, 30, 32]	Motivate for strong passwords (e.g. by explaining the goal of the training).
Design	I.3	[5]	Use self-reflection.
Design	I.4	[7, 20]	Tell about all costs and benefits directly mapped to the user.
Design	I.5	[2, 13, 14]	Easy to understand
Design	I.6	[2, 13, 14]	Plausible and applicable to the reality of the user
Design	I.7	[3, 15, 32, 35]	Indicate that recommendations may not match the user's perception.

B Email Offering the Deal

Dear colleagues,
we are aware of the burden our current password policy (minimum length of 8 characters, usage of 4 character classes, renewal after 3 months) places on you, because it is hard to create and remember a complex password every three months. We know that the current password policy leads to insecure behavior (e.g., writing the passwords on post-its), because the policy is too demanding. As a consequence, we decided to offer you a deal to make your life with passwords easier. We have modified the password policy for you according to current scientific recommendations. In return we ask you to participate in a 9-minutes training video and create a new and secure password afterwards.
From now on, the new password policy only requires a minimum length of 20 characters and the passwords will no longer expire. 20 characters sounds quite long, but we promise the new password policy will be much easier to handle for you, once you have participated in our 9-minutes training video on password security.
After you have watched the training video, we would like to ask you to change your current password for a very last time according to our new password policy. Thereafter, your password will no longer expire and you do not have to renew it again and again.
We know your time is valuable, therefore, we designed the training as short as possible for you.
Information Security is at the heart of our organization – and we would like you to make it a top priority as well.
Best regards

C User Study Questions

Table 2: Final questions of the user study.

Question ID	Question	Answer Options
PW01	How do you feel about the requirement to change your password on a regular basis?	Free text
CP03	What would you do after reading this mail?	"I would watch the mentioned training video.", "I would just change my password.", Free text
CP05	Would you comply with the request and change your password?	"Yes, I would comply and change my password.", "No, I would do the following: [free text]"
CP06	Would you follow the recommendations regarding passwords described in the video?	Yes, Partially, No
CP07	How would you implement the recommendations of the video?	Free text
CP08	Have you identified a deal or an offering in the mailing or the training video?	Yes, No
CP09	How do you feel about this deal?	Free text
CP10	How could the deal be made more obvious so that it would be more clear to you?	Free text
CP12	How could the deal be improved to give you an even greater incentive?	Free text
CP13	How did you feel about the extent or length of the mailing?	Too long, Ok, Too short
CP14	What did you find particularly good about the mailing?	Free text
CP15	What could be improved about the mailing?	Free text
CP16	What did you think of the extent of content (number of learning points) in the video?	Too many, Ok, Too few
CP17	What did you think of the duration of the video?	Too long, Ok, Too short
CP18	Was the content of the video well mediated?	Yes, Partially, No
CP19	How did you find the speaking speed of the dialogues?	Too fast, Ok, Too slow
CP20	What did you find particularly good about the video?	Free text
CP21	What could be improved about the video?	Free text
CP22	Do you have final remarks regarding the mailing or the video?	Free text