On The Systematic Development and Evaluation Of Password Security Awareness-Raising Materials

Peter Mayer
Karlsruhe Institute of Technology
peter.mayer@kit.edu

Christian Schwartz
usd AG
christian.schwartz@usd.de

Melanie Volkamer
Karlsruhe Institute of Technology
melanie.volkamer@kit.edu

ABSTRACT

Text passwords play an important role in protecting the assets of organisations. Thus, it is of the essence, that employees are well aware of possible attacks and defences. To that end, we developed a password security awareness-raising material in a systematic iterative process: The material is based on the literature on password security, feedback of independent experts, and feedback of lay-users. It was evaluated in the field with employees of three organisations. Our results show that the participating employees improved their abilities to (1) discern secure from insecure password-related behaviour in a variety of scenarios relating to different attacks and (2) assess passwords as secure or insecure. These improved abilities of the participants were still present in a retention after six months. Thus, the developed awareness-raising material contributes to improving the password-related security in organisations.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**;

KEYWORDS

Passwords, Usable Security, Awareness, User Study

ACM Reference Format:
Peter Mayer, Christian Schwartz, and Melanie Volkamer. 2018. On The Systematic Development and Evaluation Of Password Security Awareness-Raising Materials. In *2018 Annual Computer Security Applications Conference (ACSAC '18), December 3–7, 2018, San Juan, PR, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3274694.3274747

1 INTRODUCTION

Many users face problems when choosing, handling, or remembering their passwords [16, 27, 28], leading to insecure password-related behaviours. As a result, targeting passwords is the most prevalent tactic for attacks on organisations: in 2016 [32], 63% of breaches could be attributed to leveraging weak, default, or stolen passwords. In 2017 [33], this number was found to have increased to 81%.

Passwords can get into the hands of attackers in numerous ways, e.g. they can be guessed, stolen in phishing attacks, eavesdropped when communication occurs through unsecured channels, or stolen when users are observed while entering them. Many users are not aware how such attacks work and consequently how to defend against them effectively [27, 31]. Those users are at risk of falling victim to attacks, which in turn might lead to security breaches in organisations. When an organisation is affected by a breach, this can have severe financial consequences: in 2017 the average total cost of a data breach was found to be $3.62 million [25]. To prevent such consequences, it is imperative that employees of organisations understand the attacks targeting passwords and user accounts as well as the corresponding defences. The prime way to achieve this are information security awareness-raising materials [14, 35]. They are widely considered to be essential for the resilience of organisations against information security threats [19, 20]. Yet, many existing awareness-raising materials on password security demand from users an impossible task: use only complex passwords, change them frequently, and never write them down. This kind of advice is highly problematic for users [16, 27, 28] and does not represent the current state of the art [21, 37]: awareness-raising materials must effectively enable users to apply the knowledge contained within them to their daily lives or the time and effort spent working through the materials is spent in vain [2].

As core contribution of this work, we address the problem of making users aware of the different attacks on passwords and user accounts as well as defences against these attacks. To that end, we developed an awareness-raising material following an iterative process. The initial development of the material was based on research literature on password security (Section 3.1). It was then refined incorporating feedback from independent information security experts from academia and industry (Section 3.2) as well as feedback from lay-users (Section 3.3). The refined material was then evaluated in the field with employees of three organisations (Section 4). The results of our evaluation (Section 5) show that the developed material was not only received very positively and most participants found it very helpful, but it also contributes to the password-related security in organisations in two ways. Firstly, it improved the participating employees' ability to assess password-related behaviour with respect to the attacks described in the material as secure or insecure. Secondly, the participating employees improved their ability to assess the security of passwords. In particular, the results of our retention (Section 6) show that these improvements remain even six months after the participants have read through the material. From the discussion of our results, we derive some further refinements (Section 7). In summary, our awareness-raising material contributes to improving the password security in organisations. The awareness-raising material is freely available online[1], so that users and organisations can easily benefit from it.

ACSAC '18, December 3–7, 2018, San Juan, PR, USA

ACM ISBN 978-1-4503-6569-7/18/12…$15.00
https://doi.org/10.1145/3274694.3274747

[1] https://secuso.org/passwortsicherheit (in German only)

2 RELATED WORK

Information security awareness-raising materials [15] are an important tool in keeping users and organisations secure. Lin and Kunnathur [20] developed a theory of end user information security competence based a synthesis of information security literature. Their theory comprises three dimensions: "ethics and perception", "knowledge and skills", and "behaviour". They highlight information security awareness as vital part of the knowledge and skills dimension. This is further evidenced by the many studies (e.g. [7, 10, 18, 23, 26]) having identified the importance of advice and awareness-raising materials. Also, the literature review of Lebek et al. [19] identifies information security awareness as antecedent of attitude toward secure behaviour. Thus, institutions such as NIST [35] recommend organisations to distribute awareness-raising materials among their employees. Some industry standards even require it from organisations aiming to be compliant with it [24]. However, it has been found, that existing password advice often contradicts current research [21, 37]. Zhang-Kennedy et al. [37] present a review of established advice for general-purpose authentication on the web. They conclude that many existing rules (e.g. to change passwords frequently) do not represent the current state of art and propose a new set of password rules to give as advice to users. Murray and Malone [21] present an analysis of actual password advice given by different organisations on the Internet and conclude that the majority of advice contradicts the current state of research.

Due to the importance of awareness-raising materials, research literature has highlighted several important aspects of their development. Bada and Sasse [2] analysed which aspects are involved in the success and failure of security awareness campaigns. They identified as precedents to successful awareness materials the relevancy of the materials for the users and that the advice in the materials is actionable. Their recommendation is that all awareness-raising materials should pay great attention to these aspects. Tsohou et al. [30] add to these recommendations in their review of literature on cognitive and cultural biases influencing users information security perceptions and behaviours. From the reviewed literature they derive three recommendations for the development of awareness-raising materials: (1) using positive stimuli and relative frequencies to overcome affect biases, (2) the design of the material must accommodate for the fact that users tend to rely on the first piece of information they are provided with, and (3) the material should emphasise immediate consequences. Another important concept for the development of awareness-raising materials is intellectual need (also called problem-solution ordering) as described by Fuller et al. [12]. It describes the fact that learners are more motivated and effective at acquiring knowledge, when presented with the problem before the solution is explained to them. Furthermore, using expert feedback and behaviour has been identified as an important aspect in the development of advice for lay-users. Ion et al. [17] compared expert to non-expert information security behaviour to collect useful information security advice for lay-users. Their study focused on information security behaviour in general. They found that expert and non-expert behaviour differ and summarise their findings by saying that "some promising security advice emerges: (1) install software updates, (2) use a password manager, and (3) use two-factor authentication for online accounts." Likewise, Stobert and Biddle [28] conducted interviews with information security experts specifically in the context of passwords and user accounts. They find that non-experts are in need of consistent strategies to better protect themselves and that the adoption of password managers could help non-experts to manage their passwords more securely.

Focusing on the creation of concrete password security awareness-raising materials, Zhang-Kennedy et al. [36] developed three infographic posters and an online educational comic. They evaluated the posters against a text condition - "the Wikipedia description of how password cracking works" - and found that the posters with explanatory graphics were more effective in the knowledge transfer than the textual Wikipedia description, underlining the importance of graphical elements in awareness-raising materials.

3 DEVELOPMENT OF THE AWARENESS-RAISING MATERIAL

The goal of this work is to create an awareness-raising material describing possible attacks on passwords and user accounts as well as effective defences against the attacks. For the development of our awareness material we applied the recommendations of the research literature outlined in the last section.

Awareness-raising materials exist in a variety of formats [29], e.g. instructor-based, computer-based, and text-based. Each format offers different advantages and disadvantages. In this work, we focus on text-based awareness-raising materials. They allow self-paced learning, where the employees can choose the time and location of their convenience to engage in the awareness-raising materials and they can easily accommodate for reasonable breakpoints [22].

For the development of the awareness-raising material, we employed a process with three iterations. The initial iteration of the awareness-raising material was based on the literature on password security and focused on the aggregation of relevant content. This in particular addresses the detachment of password advice and current research literature described by Murray and Malone [21] as well as Zhang-Kennedy et al. [37]. The second iteration incorporated feedback gathered from experts from academia and industry. It focused on the correctness and completeness of the material's content. The third iteration added visual elements and incorporated the informal feedback of lay-users. It focused on the appeal and understandability of the material.

3.1 First Iteration - Based on Literature

The first step in the development of the awareness-raising material was the identification of relevant content. When preparing the content for the awareness-raising material, we followed the first recommendation of Tsohou et al. [30], i.e. we used positive phrasing and relative frequencies whenever possible. In addition, since our awareness-raising material specifically targets lay-users, we used non-technical terms wherever possible.

We decided to add two introductory sections giving the users a short overview of (1) who might attack them and where attacks can be targeted at and (2) the possible consequences of successful attacks. The latter is thereby intended to addresses the third recommendation of Tsohou et al. [30]. However, we carefully balanced this recommendation with the first, focusing in our awareness-material

on the positive phrasing instead of risk and fear. Thereafter, the description of the actual attacks and defences follow. Following the recommendations of Bada and Sasse [2] we strongly focused on relevant attacks on passwords and user accounts as well as actionable defences against them. The selection of attacks is based on the detailed comparative analysis of a variety of authentication schemes by Bonneau et al. [5]. In their analysis, they compare the authentication schemes' security based on eleven so-called security benefits and the corresponding attacks. In addition to the attacks in [5], we considered the exploitation of reset-mechanisms. This attack is highly relevant, since commonly used reset-mechanisms such as "personal security questions" have been shown to offer low security [4]. The defences are based on the literature on password security and included in particular the recommendations identified as important advice, e.g. by Ion et al. [17] to use password managers and two-factor authentication (cf. section 2).

The attacks in the work of Bonneau et al. [5] do not follow a systematic order. For our awareness-raising material, we ordered them in "ascending distance from the user", i.e. first attacks on the users themselves, then on the users' devices, then the communication between the devices and remote services, etc. The description of each attack was divided into three parts: a description of the attack, a description of the defences, and further hints. Thereby, we address the second recommendation of Tsohou et al. [30] by giving the most important information on each attack and defence strategy first. The dedicated *further hints*-section comes last and includes only information that we anticipate to be relevant or interesting for few users (e.g. hints for specific software).

The included types of attacks are: (a) Attacks targeted directly at the users and their interaction with their devices, e.g. based on fraudulent messages or shoulder surfing; (b) attacks targeted at the user's device through malware; (c) attacks targeted at compromising the communication between the users' devices and remote services; (d) attacks targeted at the devices and remote services (e.g. servers of a website), i.e. insecurely store passwords on users' devices and guessing attacks; and (e) attacks targeted at remote services (e.g. servers of a website). Beside the aforementioned two technologies, i.e. password managers and two-factor authentication, the awareness-raising material included also descriptions of the technologies: fingerprint readers, graphical passwords, hardware tokens, privacy filters, and single-sign-on. For a detailed overview of the awareness-raising material's content, i.e. all included attacks and technologies, see appendix A.

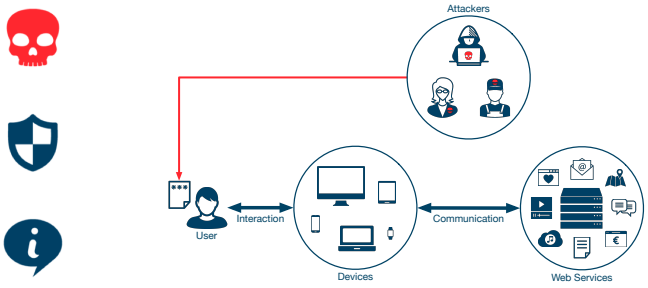
3.2 Second Iteration - Incorporation of Structured Expert Feedback

To improve the initial version of the awareness-raising material, we iterated its development based on a round of structured expert feedback. The goal of this second iteration was to ensure the awareness-raising material's completeness (i.e. aspects that would be relevant to users in the organisational and the private context) and correctness (i.e. no errors or unclear descriptions leading to the perception of errors in the content) from an information security point of view. For this purpose, we created a PDF-file of the awareness-raising material with a dedicated feedback page inserted after each of the two introductory sections as well as after the descriptions of each attack. Each feedback page had two free text questions asking (a) if the expert felt that any aspects would be missing from the description of the attack, and (b) if the expert thought that the description of the attack should be altered to be clearer. We contacted 30 independent information security experts from academia and from industry (researchers, information security consultants, etc.) and sent them the awareness-raising material with instructions to give feedback on each section. The experts were contacted based on their expertise in the password security domain and their expertise in the context of SMEs. Only German native-speakers were contacted, since our awareness-raising materials were created in German. From the 30 experts we contacted, 13 sent us their feedback. We received responses from three researchers, four IT security consultants, three IT administrators, two people working in the IT security department of their companies, and one person working in a company testing and developing security solutions. Thus, we received feedback from a diverse set of experts. In the following, we outline the major improvements to the awareness-raising material derived from the feedback.

3.2.1 More detailed information about possible consequences. Due to the focus on positive phrasing, the the first iteration of the awareness-raising material comprised only relatively few, but broad examples of possible consequences. All experts noted that more concrete examples would be beneficial. Therefore, we adjusted the focus on positive phrasing based on the structured expert feedback and expanded the respective introductory section with concrete examples of consequences of breaches for different attacks and types of user accounts (e.g. banking, email, social networks, etc.). Also, we used the expert feedback to improve the phrasing of the consequences to target more specifically employees of SMEs.

3.2.2 Split of the attacks on network communication. The majority of experts felt that the section on attacking the network communication would benefit from a split in two sections: one covering attacking unencrypted communication and one covering attacking encrypted communication. Therefore, we split up the section accordingly into one attack named "Eavesdropping on unencrypted communication" and one attack named "Eavesdropping on encrypted communication". Note that for these two attacks the wording was improved based on the expert feedback as well, replacing the term "compromising" with "eavesdropping" since it was frequently mentioned the term might be better suited for lay-users.

3.2.3 The aspect of physical access in order to compromise devices. Several experts noted that the description on how devices can be compromised should not only focus on malware, but also include physical access to the devices, e.g. accessing devices directly or tampering with them, when employees are not in the vicinity of their devices and the devices are therefore unattended. While the awareness-raising material already instructed users to set a password lock on their devices and lock the devices whenever they leave them unattended, the experts felt further scenarios were of importance (e.g. access to data on unencrypted hard drives by removing the drives from an unattended device). Consequently, we reworked the respective section to include these aspects.



(a) (b)

Figure 1: The visual elements in the awareness-raising material: (a) the icons signifying different types of content; (b) an example of the images included for each of the attacks (here: illustrating the theft of a note of a password). The image intentionally includes different types of attackers.

3.3 Third Iteration - Visual Elements and Lay-User Feedback

The third iteration focused on the visual appeal and the understandability of the awareness-raising material. We added visual elements to the material and incorporated qualitative feedback of lay-users on both, the textual descriptions and the visual elements. To this end, we met with several lay-users from our university (i.e. secretaries, designers, and project coordinators) in our lab, gave them the awareness-raising material and asked them to point out any aspect they had problems understanding or found visually unappealing. With respect to the textual descriptions, only minor changes (e.g. wording) were necessary. For the visual design, we added dedicated icons to signify the different types of content: a red skull signifying the attack description, a blue shield signifying the defence description, and a blue speech bubble with an "i" on it to signify further hints. Also, images illustrating each of the attacks were added to the attack's descriptions. Figure 1 depicts these visual elements.

4 USER STUDY METHODOLOGY

In their review of literature on information security awareness, Haeussinger and Kranz [14] recommend to evaluate awareness-raising materials in real work environments. Additionally, small and medium-sized enterprises (SMEs) seem to be a particularly interesting target for attackers: 61% of attacks in 2017 occurred in organisations with under 1000 employees [33]. Therefore, we decided to conduct our study with 90 lay-users employed in three different SMEs in their real work environments (30 participants in each SME). The main goal of this study is to evaluate the effectiveness of the awareness-raising material in conveying the knowledge regarding the attacks and defences to the users. In addition, correctly assessing the security of passwords is a crucial aspect of password management. Even when relying on password managers, users in the SME context most often have to choose some passwords themselves, in particular the master password for their password manager [37], but also the password for unlocking their workstation and other uses [16]. Therefore, we also assessed the material's effect on the participants' respective skill. Additionally, we wanted to gain qualitative feedback from the users with respect to the usefulness of the awareness-raising material and the images added in the third iteration of its development. The study methodology conforms to all requirements of our university's ethics commission. In the following, we explain in detail the hypotheses, procedure, and questionnaires of our study as well as some important aspects of the analysis methodology.

4.1 Hypotheses

To evaluate the effectiveness of the awareness-raising material, it is important to test whether the contained knowledge is actionable, i.e. the participants know how to behave in a situation of attack. To that end, typically pre-treatment and post-treatment questionnaires with the same items are used to measure the difference in performance of the participants (where the treatment is the awareness-raising material). Our respective hypothesis is:

H_{1a}: *The awareness-raising material significantly increases the users' ability to discern secure from insecure password-related behaviour in different scenarios* ***known*** *to the participant before reading through the material.*

However, a frequent criticism of such evaluations is that the pre-treatment questionnaire primes the participants with respect to the treatment. It remains therefore unknown if an improvement which is measured after the participants have read through the material can be transferred to new scenarios. Therefore, we decided to investigate not only whether participants improve their ability to discern secure from insecure password-related behaviour in scenarios known from the pre-treatment questionnaire, but to also include new scenarios to the post-treatment questionnaire. Our corresponding hypothesis is:

H_{1b}: *The awareness-raising material significantly increases the users' ability to discern secure from insecure password-related behaviour in different scenarios* ***unknown*** *to the participant before reading through the material.*

The skill of correctly assessing the security of passwords is essential to the assessment of behaviour related to password security in the face of guessing attacks, even when relying on technologies such as password managers. Our respective hypothesis is:

H_{2a}: *The awareness-raising material significantly increases the users' ability to correctly assess the security of passwords.*

The above hypotheses H_{1a}, H_{1b}, and H_{2a} pertain to the effect of the awareness-raising material observed directly after the treatment. In addition to this direct effect, it is important that the effect of the awareness-raising material does not decline even after longer periods of time, since companies will usually distribute awareness-raising material not continuously, but rather in intervals (e.g. annually, biannually, or quarterly). Therefore, we decided to also investigate the effects of the awareness raising material in a retention after six months. The respective hypotheses are

H_{1c}: *The awareness-raising material significantly increases the users' ability to discern secure from insecure password-related behaviour in different scenarios* ***known*** *to the participant before reading through the material even six months after reading it.*

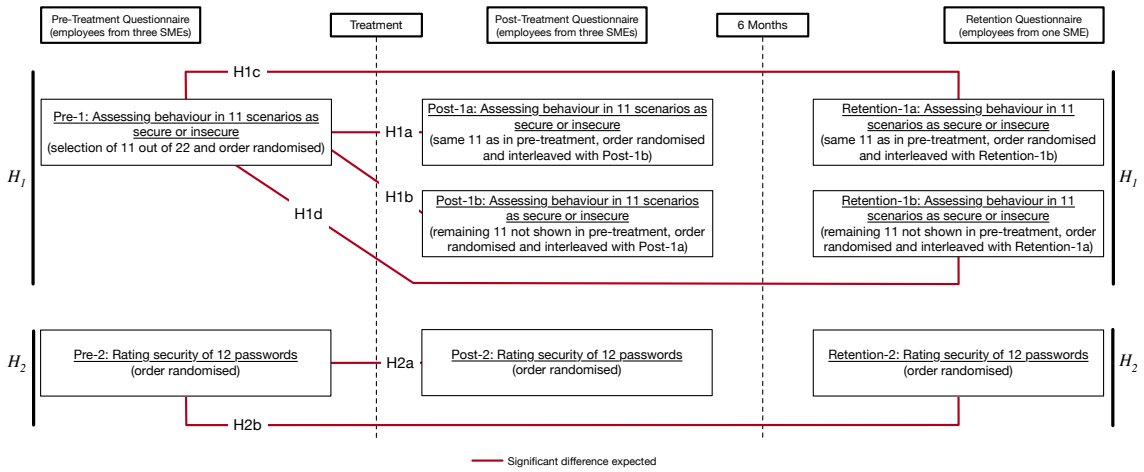


Figure 2: Overview of the study design with respect to the hypotheses in our analysis. Note that H_{1a}, H_{1b}, and H_{2a} pertain to the data collected from the participating employees of all three SMEs. Since only one SME participated in the retention after six months, H_{1c}, H_{1d}, and H_{2b} pertain only to the data collected from the participating employees from that one SME.

H_{1d}: *The awareness-raising material significantly increases the users' ability to discern secure from insecure password-related behaviour in different scenarios* ***unknown*** *to the participant before reading through the material even six months after reading it.*

H_{2b}: *The awareness-raising material significantly increases the users' ability to correctly assess the security of passwords even six months after reading it.*

4.2 Procedure

To investigate the hypotheses outlined in the last section, we employed a study procedure consisting of four phases: (1) a pre-treatment questionnaire measuring the baseline for the hypotheses in our participant sample; (2) the treatment using the developed awareness-raising material, (3) a post-treatment questionnaire measuring the effect of the treatment with respect to the aforementioned hypotheses and gathering the qualitative feedback as well as collecting basic demographics data, and (4) a retention questionnaire measuring the effect of the treatment with respect to the aforementioned hypotheses after six months. Figure 2 depicts an overview of these phases in the context of the hypotheses presented in the last section.

The evaluation was conducted with employees at three SMEs in Germany. Consequently, we conducted the user study in German, i.e. the awareness-raising material and the questionnaires were given to the participants in German. The participants were explicitly selected as lay-users with respect to information security and from a wide range of professions by a contact person in each of the three organisations. The contact person also sent out and collected the questionnaires. Using a contact person as intermediary in each organisation ensured that participants remained anonymous, despite answering the questionnaires in their real work environment. Participants received the questionnaires and the awareness-raising material as PDF-files via email one after the other as per the four phases outlined before (i.e. one PDF-file per phase). The PDF-file in the fist phase comprised the pre-treatment questionnaire with the respective instructions (overall 20 pages). The PDF-file in the second phase comprised only the awareness-raising material (overall 110 pages). The PDF-file in the third phase comprised the post-treatment questionnaire with the respective instructions (overall 42 pages). The PDF-file in the fourth phase comprised the retention questionnaire and the respective instructions (overall 30 pages). Only upon sending the completed pre-treatment questionnaire, the participant received the awareness-raising material with the instruction to take their time to read it. Once the participants confirmed that they had read the awareness-raising material, they received the post-treatment questionnaire. After all participants in an organisation had completed the post-treatment questionnaires, the contact person sent the filled-out questionnaires to the authors. Then, after six months the contact person received the retention questionnaires for all participants and again sent the filled ones back to us. Only one of the SMEs agreed to participate in the retention session. This is further discussed in section 7.

4.3 Questionnaires

In this section, we present the items used in our evaluation. All items were developed in an iterative process using feedback from psychologists and from two rounds of pre-tests with lay-users.

For H_{1a-d} 22 scenarios were developed to evaluate the participants' ability to correctly assess specific password-related behaviour as secure or insecure. For each of the 11 attacks described in section 3, two scenarios were developed: one representing secure behaviour and one representing insecure behaviour. The scenarios were developed with additional feedback from information security consultants, in order to increase the real world relevancy of the scenarios for SME employees. The scenarios are closely aligned with the attacks and defences described in the awareness-raising material. Thereby, our goal was to create challenges for the participants that did not simply test the declarative knowledge. Instead, we created scenarios that required the participant to judge password-related behaviour aligned to the attacks and defences as secure

or insecure in the same way they would have to judge their own behaviour when applying the newly gained knowledge in different situations of their daily lives. An overview of all 22 scenarios can be found in table 2 in the appendix at the end of this paper. In the questionnaires, each scenario was accompanied by two questions: (1) a binary question where the participants had to indicate whether they believed the scenario represents secure or insecure behaviour and (2) an open text question offering the participants the possibility to justify their decision.

To allow testing H_{1a-d} using the developed scenarios, the pre-treatment questionnaire comprised only 11 of the 22 scenarios chosen at random for each participant (one for each of the attacks, balanced in terms of secure/insecure behaviour). The post-treatment questionnaire comprised all 22 scenarios. This allowed us to assess not only the performance in scenarios known before the treatment, but also the participants' ability to transfer the gained knowledge to new scenarios. The retention questionnaire also included all 22 scenarios. The order of the scenarios was randomised for each participant in all questionnaires.

For $H_{2a,b}$, the participants had to rate 12 passwords according to their security on a 5-point Likert scale (see Figure 3 on the next page for the full list). Only the two ends of the scale were labelled as *very insecure* and *very secure*. Of the 12 passwords, seven were chosen to be guessable within seconds using Hashcat with the best64 and generated2 rule sets in conjunction with Mark Burnett's wordlist [8] which he specifically released for academic research (in the following "insecure passwords"). The remaining 5 passwords were chosen using a German diceware list (about 80'000 entries, created from the German Mozilla Firefox dictionary) to be not guessable with reasonable effort (in the following "secure passwords"). All 12 passwords were included in all three questionnaires.

With respect to the qualitative feedback, we asked free text questions regarding four aspects: (1) the relevancy of the included information (item: "Was the content of the awareness-raising material relevant for you?"); (2) additional information the participants would have hoped for (item: "Which additional information would you have hoped for in the awareness-raising material?"); (3) helpfulness of the images for understanding the content of the awareness-raising material (item: "Were the images helpful in understanding the content of the awareness-raising-material? How could they be improved?"); and (4) whether the awareness-raising material will have an effect on how the participants manage their passwords and, if so, what effect it is (item: "Will the content of the awareness-raising material influence the way you currently manage your passwords?"). As demographics, we only collected the participants' gender and age. The qualitative questions inquiring the participants' opinion on the awareness-raising material's content and visual elements (as well as the demographics questions) were only present in the post-treatment questionnaire.

4.4 Analysis

Due to the fact, that only employees from one SME filled the retention questionnaires, the size of the sample is also reduced to a third. Therefore, we first present the analysis of the results of the pre-treatment and post-treatment questionnaires (i.e. $H_{1a,b}$ and H_{2a}) in section 5. Thereafter, we present the results of the retention questionnaires (i.e. $H_{1c,d}$ and H_{2b}) in section section 6.

For the analyses pertaining to the assessment of behaviour in scenarios related to password security, the participants responses were aggregated into ratios of correct responses for each scenario. Thereby, it is important to note that H_{1a} and H_{1c} are thus based on a within-subject design: all responses pertaining to scenarios not seen by the respective participant in the pre-treatment questionnaire are excluded from the post-treatment questionnaire data in this analysis. Consequently, paired hypothesis tests are used in this case. In contrast, the analyses of H_{1b} and H_{1d} are based on a between-subjects design: the responses in the post-treatment questionnaire stem solely from participants that have not seen the respective scenarios in the pre-treatment questionnaire. Consequently, independent sample hypothesis tests are used in this case. Since our data was not normally distributed we used the non-parametric Wilcoxon signed rank test for paired samples and the non-parametric Wilcoxon rank sum test for independent samples. We used Bonferroni-Holm-corrected α-levels where appropriate. Effect sizes are interpreted according to [9] as small ($r \geq 0.10$), medium ($r \geq 0.30$) or large ($r \geq 0.50$).

5 RESULTS – PRE-TREATMENT AND POST-TREATMENT QUESTIONNAIRES

In this section, we present the results of our analysis of the data pertaining to the pre-treatment and post-treatment questionnaires. Overall 90 employees from three SMEs in Germany filled the pre-treatment and post-treatment questionnaires. Six participants had to be excluded from the analysis. Their answers to the free text questions showed detailed knowledge of information security (e.g. different encryption algorithms) and therefore raised doubts as to whether they would qualify as lay-users. Of the remaining 84 participants, 56 were male, 27 were female, and one participant chose to not answer this question. The participants' age ranged from 19 years to 43 years (M: 30.0 years; SD: 5.4 years).

5.1 Assessment of Scenarios

For most scenarios, the participating employees assessed the described behaviour correctly in the pre-treatment questionnaire. Two scenarios (3 and 13) stood out due to large numbers of incorrect answers. A large portion of the free text answers to these two scenarios indicated that specific formulations in the scenarios caused participating employees to misinterpret them. This indicates methodological problems with the scenarios (as opposed to problems with the content of the awareness-raising material), which were not uncovered in the pre-tests. For scenario 3, the majority of participants perceived a locked drawer at home not as secure storage. For scenario 13, the majority of participants perceived that a dog's birthday would not be a secret, despite the scenario explicitly stating this as fact. Thus, we excluded these two scenarios from the analysis and only the responses to the remaining 20 scenarios were considered. An overview of the results is depicted in Figure 3a.

5.1.1 Analysis of H_{1a}. The awareness-raising material leads to an overall increase in correctly assessed scenarios from 88.2% before the treatment to 93.3% afterwards, when considering the responses with respect to the scenarios participants saw before and after the

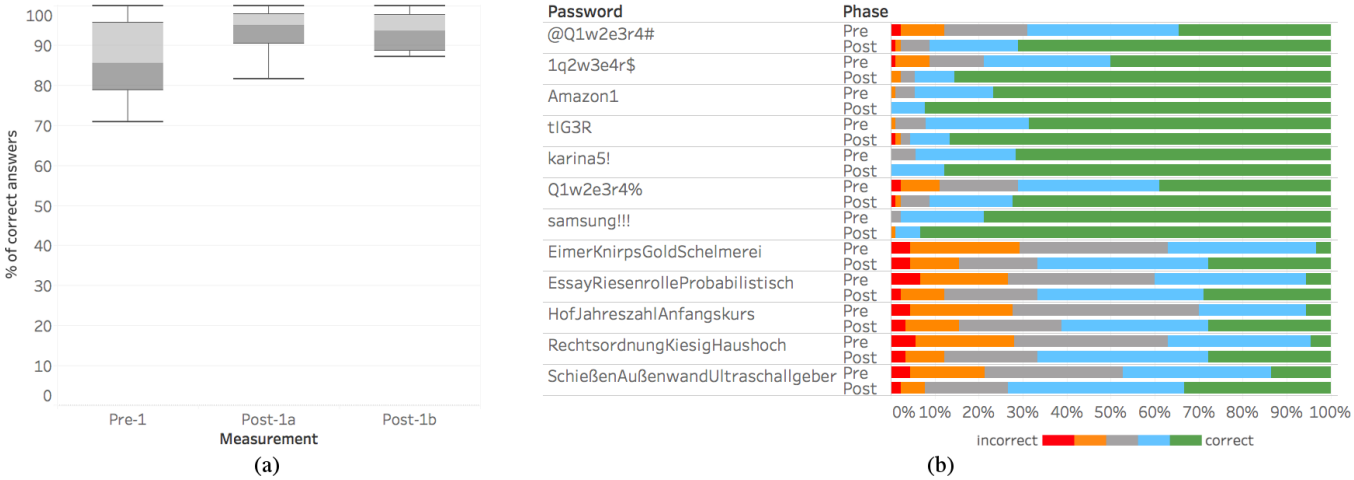


Figure 3: Overview of the results from the pre-treatment and post-treatment questionnaires. (a) Overview of the ratios of correct responses to the scenarios for the pre-treatment and post-treatment questionnaires. (b) The responses on the 5-point Likert scale with respect to the perceived security. In this chart, the participants' responses are equalised in terms of correctness: the higher the value, the more correct (i.e. insecure for the easy to guess passwords and secure for the diceware passwords) is the participants' assessment.

treatment (Pre-1 and Post-1a in Figure 2). A Wilcoxon signed rank test shows this increase to be significant ($V = 25.5$, $p = .017$). The effect size $r = 0.378$ is above .3, i.e. indicates a medium effect. This indicates that working through the awareness-raising material leads to a significant improvement in the employees' ability to assess behaviour as secure or insecure in scenarios known before the treatment. Thus, the results of our study support H_{1a}.

5.1.2 Analysis of H_{1b}. Additionally, we investigate whether the participants can transfer the knowledge gained by reading the awareness-raising material to scenarios they only saw in the post-treatment questionnaire. A Wilcoxon rank sum test does not find a significant difference ($W = 134$, $p = .070$) between the portions of correct responses in the pre-treatment questionnaire and the responses in the post-treatment questionnaire corresponding to the scenarios only present in the post-treatment questionnaire (Pre-1 and Post-1b in Figure 2). While the test only closely fails significance, this result indicates that working through the awareness-raising material might not improve the employees' ability to assess information security behaviour as secure or insecure in new scenarios unknown before reading the awareness-raising material. Thus, the results of our study do not support H_{1b}.

5.2 Password Security Ratings

Figure 3b shows the participants' ratings of the passwords in the pre-treatment and the post-treatment questionnaires. We could only include 81 participants in the analysis regarding H_{2a}, since three participants did not complete the ratings of all passwords.

5.2.1 Analysis of H_{2a}. After the treatment, the assessment of all passwords improved, i.e. the insecure passwords were perceived as insecure by more participants and the secure passwords were perceived as secure by more participants. A Wilcoxon signed rank test showed a significant difference between the accumulated Likert scores of the 81 participants ($V = 291$, $p < .001$). The effect size $r = 0.423$ is above .3, i.e. a medium effect. Thus, the results of our study provide supporting evidence with respect to H_{2a}.

In the pre-treatment questionnaire, the security of most of the insecure passwords was assessed correctly by the participants. In contrast, the security of the secure passwords was mostly assessed incorrectly. A Wilcoxon signed rank test showed a significant difference in the correctness of the assessment between the secure and insecure passwords ($V = 3321$, $p < .001$). The effect size $r = 0.614$ indicates a large effect. This difference remains in the post-treatment questionnaire: a Wilcoxon signed rank test showed a significant difference ($V = 3240$, $p < .001$). The effect size $r = 0.612$ again indicates a large effect.

5.3 Qualitative Results

While most participants answered the qualitative questions, the participants' responses to these questions were very concise. However, for all four aspects under investigation clear themes emerged.

5.3.1 Relevancy of Included Information. Most participants who answered the respective free text questions found the content of the awareness-raising material relevant and helpful (90.6%). Participants were unexpectedly explicit with respect to their positive opinion about the material, e.g.: *"It was very helpful. I have learned a lot!"* (P7) and *"I believe the [content of the material] is relevant for everybody in today's world. I have never seen such good education materials, all information was very helpful."* (P62).

Three topics were perceived as particularly helpful by the participants: (1) the information regarding password composition and guessing attacks, (2) the information with respect to regular changes of passwords, and (3) the information on password managers. The most frequently voiced concern (stated by 6 participants) was that the awareness-raising material was perceived as too long.

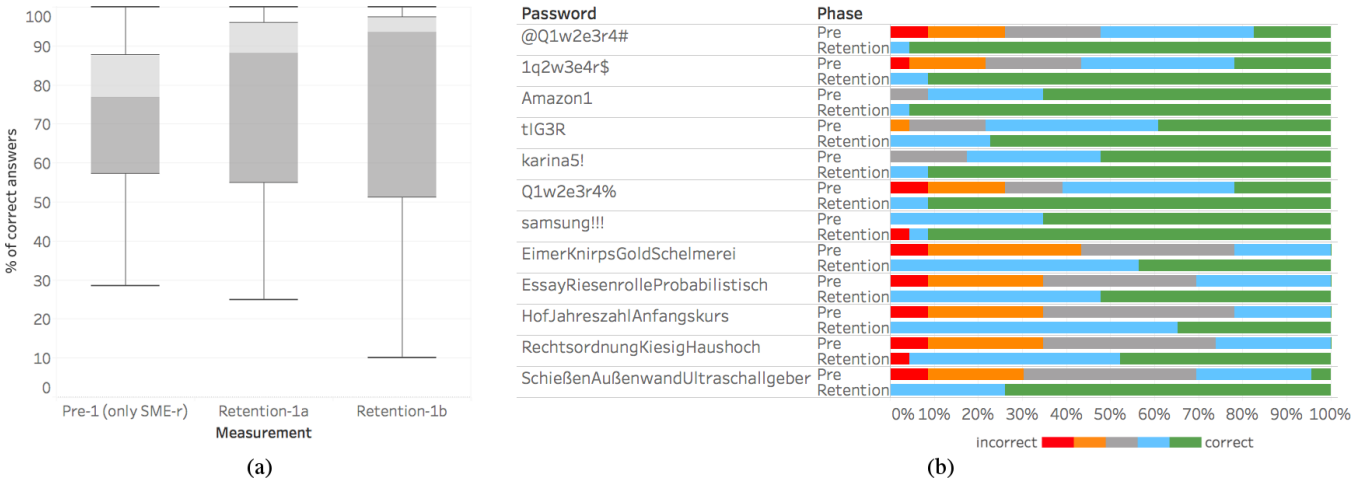


Figure 4: Overview of the results from the pre-treatment and retention-treatment questionnaires (all data only from participants of SME-r). (a) Overview of the ratios of correct responses to the scenarios for the pre-treatment and retention-treatment questionnaires. (b) The responses on the 5-point Likert scale with respect to the perceived security. In this chart, the participants' responses are equalised in terms of correctness: the higher the value, the more correct (i.e. insecure for the easy to guess passwords and secure for the diceware passwords) is the participants' assessment.

5.3.2 Additional Information the Participants Would Have Hoped For. The most frequently mentioned aspect participants would have hoped for (20.8% of participants who answered this free text question) was more concrete information with respect to password managers and software which can be used to generate passwords, e.g.: *"Concrete suggestions regarding software which can be used to generate secure passwords, about good password managers."* (P78). The participants also would have liked more concrete rules on how to choose passwords in addition to the composition advice already present in the awareness-raising material (16.7%).

5.3.3 Helpfulness of the Images. All of the participants found the images in the awareness-raising material helpful, e.g.: *"The images were very helpful in understanding the [awareness-raising material's content]."* (P53) and *"The images were very helpful."* (P89).

5.3.4 Effect of the Awareness-Raising Material on the Users' Password Management. The dominant theme in the answers to this free text question were password managers. 20.3% of participants answering this question stated their intention to start using a password manager in the future instead of their original strategy. In addition, 61.0% stated to continue using a password manager. An additional 9.8% stated to create their passwords differently from now on (without explicitly specifying in which way). The remaining 8.9% of participants answering this question stated that the awareness-raising material would have no impact on their behaviour and did not mention the use of password managers.

6 RESULTS – RETENTION QUESTIONNAIRES

In this section we present the analysis regarding the hypotheses $H_{1c,d}$ and H_{2b} based on the data from the retention questionnaires. Since only one of the three SMEs agreed to participate in the retention after six months, we highlight any differences between the SME partaking in the retention (SME-r in the following) and the other two SMEs in order to allow correct interpretation of the following analyses. Participants who had been excluded from the analysis of the pre-treatment and post-treatment questionnaires were also excluded from the analysis of the retention. Overall, the sample for the retention questionnaire comprised 26 participants. Of those 26 participants, 16 were male, 9 were female, and one participant chose to not answer this question. The participants' age ranged from 19 years to 43 years (M: 32.2 years; SD: 5.5 years).

6.1 Assessment of Scenarios

For the analysis of the retention we again excluded scenarios 3 and 13, due to their issues outlined in section section 5.1.

6.1.1 Differences of SME-r and the other two SMEs. The employees of SME-r did not perform significantly different in the pre-treatment questionnaire than the employees of the other two SMEs. A Wilcoxon rank sum test does not indicate a significant difference ($W = 151$, $p = 0.182$). This holds for the post-treatment questionnaire as well, where a Wilcoxon rank sum test also does not indicate a significant difference ($W = 207$, $p = .856$).

6.1.2 Analysis of H_{1c}. The participants of our retention perform better in the retention questionnaire than in the pre-treatment questionnaire with respect to the scenarios seen in the pre-treatment questionnaire. A Wilcoxon signed rank test indicates a significant difference ($V = 15.5$, $p = .022$) and $r = 0.363$ indicates a medium effect for this difference. Thus, the results of our study support H_{1c}. An overview of the results is depicted in figure 4a.

6.1.3 Analysis of H_{1d}. For the scenarios not seen in the pre-treatment questionnaire, assessments in the retention improved as well when compared to the pre-treatment questionnaire. A Wilcoxon rank sum test indicates a significant difference ($W = 125$,

Table 1: Overview of the results of the hypothesis tests

Hypothesis	Result	Effect Size r
Assessment of Scenarios		
H_{1a}	supported	0.378 (medium)
H_{1b}	not supported	-
H_{1c}	supported	0.363 (medium)
H_{1d}	supported	0.482 (medium)
Password Security Ratings		
H_{2a}	supported	0.423 (medium)
H_{2b}	supported	0.603 (large)

$p = .031$) and an effect size of $r = 0.482$ indicates a medium effect. Thus, the results of our study support H_{1d}.

6.2 Password Security Ratings

Note that we could only include 23 participants in the analysis regarding H_{2b}, since three of the 26 participants did not complete the ratings for all passwords.

6.2.1 Differences of SME-r and the other two SMEs. The employees of SME-r performed worse in the pre-treatment questionnaire than the employees of the other two SMEs. A Wilcoxon rank sum test showed a significant difference ($W = 405$, $p = .004$). An effect size of $r = 0.484$ indicates a medium effect. This difference between SME-r and the other two SMEs reverses in the post-treatment questionnaire: the employees of SME-r rate the security of passwords more correctly than the employees of the other two SMEs. A Wilcoxon rank sum test indicates this difference to be significant ($W = 977.5$, $p = .002$). An effect size of $r = 0.484$ indicates a medium effect.

6.2.2 Analysis of H_{2b}. A Wilcoxon rank sum test indicates that the performance in the pre-treatment questionnaire is significantly worse than in the retention questionnaire ($V = 0$, $p < .001$). An effect size of $r = 0.603$ indicates a large effect. Thus, the results of our study support H_{2b}. An overview of the results is depicted in figure 4b. Also, a Wilcoxon signed rank test showed a significant difference in the correctness of the assessment between the secure and insecure passwords for the retention questionnaire ($V = 129$, $p = .002$). An effect size of $r = 0.462$ indicates a medium effect.

7 DISCUSSION

The awareness-raising material was received positively by all participating employees and addresses all attacks deemed relevant by the literature and independent information security experts from academia and industry. Table 1 summarises the results with respect to all hypotheses in our analysis. It significantly increased the participants' ability to correctly assess the security of passwords. Moreover, it significantly increased the participants' ability to correctly assess whether password-related behaviour in different information security scenarios known before reading through the material is secure or insecure. The results regarding whether the material improves the ability to correctly assess password-related behaviour in previously unknown scenarios closely fail significance. This again shows how difficult it is to develop effective awareness-raising materials, even when following a thorough methodology during their creation. Interestingly, the results of the retention show that participants improved their ability to assess these scenarios. This might indicate that our participants talked about the different scenarios with colleagues also participating our study, that they revisited the awareness-raising material, or that there was a learning effect among the previously unknown scenarios where the later seen scenarios in the post-treatment questionnaire helped the participants to correctly assess other scenarios in the retention.

In the following, we will discuss first the improvements to the awareness-raising material we could derive from the results of our user study. Then, we discuss the limitations of this work.

7.1 Improvements Derived from the User Study

Despite the overall successful outcome of this work, we identify four areas for further improvements.

Firstly, the poor performance of the participants with respect to one of the scenarios (scenario 9) mandated a further improvement to the awareness-raising material. Fortunately, the free text answers offered an explanation for the poor performance and the respective formulation in the material could be adapted. Due to the fact that we wanted to leave it up to the participants whether or not to revisit the material before the retention questionnaire, this correction is not yet visible in the retention results. However, the corrections were later made available to the participating employees.

Secondly, participants seemed to be hesitant to rate the security of long passwords composed of multiple concatenated words correctly. In contrast, our participants could significantly better identify insecure passwords. This seems to indicate that our awareness-raising material was more effective in improving the ability of the participants to recognise insecure passwords than the ability to recognise secure ones. Therefore, one focus of further improvements must be the teaching of good creation strategies. As a first step, we added additional explanations and examples to the respective sections of the material. Again, the additional explanations and examples were only available to the participants after the retention.

Thirdly, the qualitative answers show that the participating employees desire additional concrete advice with respect to two aspects: (1) how to create secure passwords and (2) password managers. The former should be addressed to some degree by the information added to the awareness-raising material as outlined in the last paragraph. Yet, a section dedicated to password creation strategies should be considered in future iterations of the material. Need for the latter is also supported by the large number of participants who stated that they would start using a password manager after having worked through the material. This is a positive effect, as usage of password managers is widely considered a good advice to users by information security experts [17, 28].

Lastly, the awareness-raising material currently includes only the technologies: password managers, two-factor authentication, fingerprint readers, graphical passwords, hardware tokens, privacy filters, and single-sign-on. Future versions of the awareness-raising material might need to include additional alternatives to text passwords should they gain widespread adoption (e.g. Face ID [1] or palm vein authentication [3]).

Despite the need for further improvements as outlined above, we argue that this work can help create awareness-raising materials beyond the original application in the password context. The iterative process used to create the password security awareness-raising material could be easily applied to other information security contexts, further contributing to the information security in organisations. Therefore, applying the process in areas other than password security represents one important line of future work.

7.2 Limitations

One limitation of our user study lies in the participant sample. While the contact persons assured us that all participants would be lay-users with respect to information security, we had to exclude six participating employees, since their responses to the free text answers indicated a thorough knowledge of information security. Also, all participants are employed in German SMEs. Consequently, it is unclear whether our findings fully translate to different groups of users and to different countries. As future work, we plan to validate our results in various contexts.

Following the recommendations of Haeussinger and Kranz [14], we conducted the study in the real work environments of the participating employees. The most reliable option in this regard would have been to monitor the password-related behaviour of the employees in their organisation and check whether the awareness-raising material influences this behaviour. However, such a design has severe issues in a real world setting in organisations: Gathering the necessary data might pose security risks (e.g. passwords created by the employees to see whether creation strategies change) or have legal and privacy implications (e.g. surveilling employees at their desks in order to see whether they store notes of passwords insecurely). Consequently, we chose a different study design, allowing us to retain the anonymity and privacy of our participants as well as avoid any security risks, while delivering the study materials to the participants' real work environments. However, this design came with the trade-off that contact to the participants was only possible through the contact persons. Thus, the study setting could not be controlled. The participants were unsupervised throughout all four phases of the study. Therefore, a number of limitations arise: (a) participants might have used the material while filling out the questionnaire, (b) participants might have filled out the post-treatment questionnaire after reading the material only partially, (c) participants who work in the same SME might have worked (partially) together, and (d) participants might have spent very different amounts of time reading through the material which might have impaired consistency not only between organisations, but also between the participants of each organisation. To counteract these issues, participants received instructions during each of the four phases in our study. Participants were instructed to read the awareness-raising material carefully and in its entirety. Also, they were told that the post-treatment questionnaire would be sent out only after they had explicitly acknowledged having read the entire material. Last but not least, participants were instructed to fill out the questionnaire by themselves.

Furthermore, only one of the three SMEs agreed to participate in the retention after six months. Concerns in the SMEs focused mostly on the potential impact on productivity, due to the participants filling out the questionnaires in their working environment. This was a huge factor deterring SMEs from participating in the study. While addressing this issue is difficult, since thorough investigations rely on thorough questionnaires, we advise any researcher planning similar endeavours to consider this issue.

Another limitation relates to the baseline in our participant sample. Even before working through the material, over 88% of the responses were correct. This might indicate (a) a methodological problem resulting from misaligned difficulty levels of the scenarios or (b) that the participants in our sample had already received education with respect to password security before our study. Studies with more difficult scenarios and different samples are needed to investigate which of the two represents the cause for this issue.

Finally, we could not include a control condition in our study design due to the limited amount of participants we could recruit in the SMEs although this would have allowed us to present stronger evidence with respect to the effectiveness of our awareness-raising material.

8 CONCLUSION

In this work, we present a novel and systematically developed awareness-raising material to make lay-users aware of attacks on passwords and user accounts as well as the respective defences. We developed this awareness-raising material in an iterative process. It addresses all attacks deemed relevant by the literature and independent information security experts from academia and industry. It increases the participants' ability to correctly assess (a) whether specific password-related behaviour in different information security scenarios is secure or insecure and (b) the security of passwords. In particular, these abilities are retained or even improved six months after reading through the awareness-raising material. At the same time, the awareness-raising material was received positively by all participants.

The results of our study also point out areas for future work. The participating employees expressed the desire to learn more about password managers and the composition of secure passwords. Thus, it might be warranted to create additional awareness-raising materials for these topics. Also, it might be worthwhile to investigate how to make the transition towards using a password manager easier for users. Beyond the scope of password security, the iterative process used to systematically create the awareness-raising material presented in this work could easily be applied to other information security contexts.

ACKNOWLEDGEMENTS

We would like to thank all experts and participants. Also, we would like to thank our reviewers and our shepherd for their insightful comments and feedback, which helped to greatly improve this paper. This work has been developed by the authors at Technische Universität Darmstadt within the project 'KMU AWARE' which was funded by the German Federal Ministry for Economic Affairs and Energy. 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).

REFERENCES

[1] Apple Inc. 2017. *Face ID Security.* Technical Report.
[2] Maria Bada and Angela Sasse. 2014. *Cyber Security Awareness Campaigns - Why do they fail to change behaviour?* Technical Report.
[3] Christian Bock. 2018. Fujitsu and Microsoft focused on advancing security in the modern workplace. https://blogs.windows.com/business/2018/02/08/fujitsu-microsoft-focused-advancing-security-modern-workplace/
[4] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. 2015. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In *International Conference on World Wide Web*. 141–150.
[5] Joseph Bonneau, Cormac Herley, Paul C van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE Symposium on Security and Privacy*. 553–567.
[6] Joseph Bonneau, Mike Just, and Greg Matthews. 2010. What's in a Name?. In *International Conference on Financial Cryptography and Data Security*. 98–113.
[7] B Bulgurcu, H Cavusoglu, and I Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* (2010).
[8] Mark Burnett. 2015. Today I Am Releasing Ten Million Passwords . https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495
[9] J Cohen. 1988. Statistical power analysis for the behavioral sciences (2nd ed.). *Academic Press* (1988).
[10] Mete Eminağaoğlu, Erdem Uçar, and Şaban Eren. 2009. The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report* 14, 4 (Nov. 2009), 223–229.
[11] Dinei Florêncio, Cormac Herley, and Paul C van Oorschot. 2014. An Administrator's Guide to Internet Password Research. In *Large Installation System Administration Conference*. 35–52.
[12] Evan Fuller, Jeffrey M Rabin, and Guershon Harel. 2011. Intellectual Need and Problem-Free Activity in the Mathematics Classroom. *International Journal for Studies in Mathematics Education* 4, 1 (2011), 80–114.
[13] Paul A Grassi, James L Fenton, Elaine M Newton, Ray A Perlner, Andrew R Regenscheid, William E Burr, Justin P Richter, Naomi B Lefkovitz, Jamie M Danker, Yee-Yin Choong, Kristen K Greene, and Mary F Theofanos. 2017. *Digital Identity Guidelines: Authentication and Lifecycle Management.* Technical Report.
[14] Felix Haeussinger and Johann Kranz. 2017. Antecedents of Employees' Information Security Awareness - Review, Synthesis, and Directions for Future Research. In *European Conference on Information Systems*. 1–20.
[15] Norman Hänsch and Zinaida Benenson. 2014. Specifying IT Security Awareness. *Database and Expert Systems Applications (DEXA), 2014 25th International Workshop on* (2014), 326–330.
[16] Philip G Inglesant and M Angela Sasse. 2010. The true cost of unusable password policies. In *Conference on Human Factors in Computing Systems*. 383–392.
[17] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Symposium on Usable Privacy and Security*. 327–346.
[18] Miranda Kajtazi and Burcu Bulgurcu. 2013. Information Security Policy Compliance: An Empirical Study on Escalation of Commitment. In *Americas Conference on Information Systems*.
[19] Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, and Michael H Breitner. 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review* 37, 12 (2014), 1049–1092.
[20] Canchu Lin and Anand S Kunnathur. 2013. Toward Developing a Theory of End User Information Security Competence. In *Americas Conference on Information Systems*. 1–10.
[21] Hazel Murray and David Malone. 2017. Evaluating password advice. In *Irish Signals and Systems Conference*.
[22] Stephan Neumann, Benjamin Reinheimer, and Melanie Volkamer. 2017. Don't Be Deceived: The Message Might Be Fake. In *International Conference on Trust and Privacy in Digital Business*. 199–214.
[23] Gizem Öğütçü, Özlem Müge Testik, and Oumout Chouseinoglou. 2016. Analysis of personal information security behavior and awareness. *Computers & Security* 56 (Feb. 2016), 83–93.
[24] PCI Security Standards Council LLC. 2016. Payment Card Industry (PCI) Data Security Standard (Version 3.2).
[25] Ponemon Institute. 2017. *2017 Cost of Data Breach Study - Global Overview.* Technical Report.
[26] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53 (2015), 65–78.
[27] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords . In *Symposium on Usable Privacy and Security*. 243–255.
[28] Elizabeth Stobert and Robert Biddle. 2015. Expert Password Management. In *International Conference on Passwords*. 3–20.
[29] Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann. 2016. Teaching Phishing-Security: Which Way is Best? In *ICT Systems Security and Privacy Protection*. 135–149.
[30] Aggeliki Tsohou, Maria Karyda, and Spyros Kokolakis. 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security* 52 (July 2015), 128–141.
[31] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. " I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Symposium on Usable Privacy and Security*. 123–140.
[32] Verizon. 2016. *2016 Data Breach Investigations Report.* Technical Report.
[33] Verizon. 2017. *2017 Data Breach Investigations Report.* Technical Report.
[34] Melanie Volkamer, Karen Renaud, Benjamin Maximilian Reinheimer, Philipp Rack, Marco Ghiglieri, Peter Mayer, Alexandra Kunz, and Nina Gerber. 2018. Phishing Detection: Developing and Evaluating a Five Minutes Security Awareness Video [in press]. In *Proceedings of the 15th International Conference on Trust, Privacy and Security in Digital Business - TrustBus 2018, Regensburg, 5.-6. September 2018.*
[35] Mark Wilson and Joan Hash. 2003. *Building an Information Technology Security Awareness and Training Program.* Technical Report 800-50. National Institute of Standards and Technology.
[36] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2013. Password advice shouldn't be boring: Visualizing password guessing attacks. In *eCrime Researchers Summit*.
[37] Leah Zhang-Kennedy, Sonia Chiasson, and Paul van Oorschot. 2016. Revisiting Password Rules: Facilitating Human Management of Passwords. In *APWG Symposium on Electronic Crime Research*.

APPENDIX A: DESCRIPTION OF THE AWARENESS-RAISING MATERIAL

The awareness-raising material ensures understandability for lay-users by preventing technical terms, using simple language and employing a wide range of examples. Due to space constraints it is not possible to reproduce the full awareness-raising material while retaining these measures. We can provide only a high-level summary. However, the improved version of the awareness-raising material can be freely accessed online[2].

Accounting for the domain-knowledge of the readership of this article, more technical terms are used in describing the content of the awareness-raising material while also forgoing most of the examples for the sake of brevity. The remainder of this section reproduces the general structure of the awareness-raising material and provides a short description of each section.

A.1 Introductory Sections

The awareness-raising material includes two introductory sections. They give the users a short overview of (1) who might attack them and where attacks can be targeted at and (2) the possible consequences of successful attacks.

A.1.1 Possible Attackers. This section provides an overview of possible attackers, including criminal hackers, social engineers attempting to gain entry to a business facility, insider threats, spouses and acquaintances, as well as employees of IT-service providers. Next, it is explained where such attackers target their attacks, i.e. the user itself, end devices, interactions with end devices, communications between end-devices and services as well as only at services.

A.1.2 Possible Consequences of Successful Attacks. Here, the goals of attackers are discussed, thereby addressing the third recommendation of Tsohou et al. [30], i.e. emphasising consequences. However, we carefully balanced this recommendation with their

[2] https://secuso.org/passwortsicherheit (in German only)

first recommendation, focusing in our awareness-material on the positive phrasing instead of risk and fear. The user is informed that the primary goal of an attacker is not necessarily obtaining access to a user's account. Rather, attackers are interested in manipulating an account for their specific gains. Examples include accessing the victims email account in order to send phishing emails to the user's contacts, accessing cloud storage in order to blackmail the user, and accessing the users bank account in order to withdraw funds.

A.2 Attacks

This section explains the different types of attacks. The description of each attack comprises three parts: a general description of the attack, a description of the defences, and (where necessary) further hints which are only relevant for few users (e.g. hints for specific software).

A.2.1 Attack: Fraudulent messages.

Description of Attack. The attacker sends a message encouraging the victim to either provide user credentials, follow a link to a malicious website or open a malicious attachment.

Description of Defences. Participants are encouraged to delete messages identified as dangerous, verify both the sender as well as the content regarding plausibility and analyse links and attachments regarding whether they potentially represent a danger. Further, the participant is referred to specific training material concerning fraudulent messages [22].

Further Hints on the Attack. Interested participants are provided with a link to a video explaining further details regarding fraudulent messages [34]. The interested reader can find the video online[3].

A.2.2 Attack: Theft of an insecurely stored note of the password.

Description of Attack. Attackers attempt to obtain credentials stored physically in an insecure manner (e.g. a post-it under the keyboard).

Description of Defences. Physical copies of passwords should be stored securely.

Further Hints on the Attack. The participant is informed that passwords transmitted via snail-mail are also subject to attack, since they also represent a note of the password. Users should be weary when passwords delivered via mail arrive in a damaged envelope. In such cases they should be invalidated resent.

A.2.3 Attack: Shoulder-Surfing.

Description of Attack. The attacker watches the user entering his or her passwords or unlock gestures either in person or via tools such as cameras or infrared cameras.

Description of Defences. Participants are encouraged to ensure that no third party can watch them while entering credentials. Additionally, this risk can be mitigated by employing privacy filters and cleaning touch screens.

[3]https://secuso.org/video-online-fraud

A.2.4 Attack: Compromising the user's devices.

Description of Attack. The attacker attempts to compromise the users device using malware, allowing the attacker to retrieve all credentials used on the device. This might be attempted by obtaining access to an unlocked and unobserved device or by tricking the user into installing it, e.g. by accessing a website containing a drive-by download. Users of mobile devices should be aware that even Apps distributed via official App Stores may contain malware.

Description of Defences. Participants are encouraged to install all relevant security patches for their devices, e.g. by enabling automatic updates, and to consider installing anti-virus software. In addition, devices should be protected via a password (or an equivalent authentication scheme using tokens or biometrics) and not be left unattended. Further, full-disc encryption should be enabled. Users are also advised to not connect external storage media from unknown sources and to not install software from non-trusted sources. Mobile devices should not be *rooted* or *jailbroken*.

Further Hints on the Attack. The interested participant is provided with further information regarding the dangers of *rooting* or *jailbeaking* devices.

A.2.5 Attack: Eavesdropping on unencrypted communication.

Description of Attack. Attackers attempt to eavesdrop on unencrypted communication in order to obtain user credentials. This is especially easy if unencrypted WiFi networks are used or the authentication to a WiFi network occurs via an unencrypted connection. Secondary credentials such as cookies which may be transmitted via unencrypted channels may also be used by attackers to access services.

Description of Defences. Participants are encouraged to ensure that web-services are accessed via HTTPS connections and are provided with identifying features of such connections. Further, they are encouraged to logout from web-services after use in order to invalidate secondary credentials.

Further Hints on the Attack. Links to additional information in the form of videos and articles are provided to the user as well as browser plug-ins which notify users of unencrypted connections.

A.2.6 Attack: Eavesdropping on encrypted communication.

Description of Attack. Attackers attempt to impersonate remote services or perform a man-in-the-middle attack to intercept encrypted communication between the user and a service. Such attacks render the encryption useless.

Description of Defences. Users are informed about the meaning of browser warnings for insecure HTTPS connections. It is explained how to identify low risk warnings (e.g. expired certificates). Participants are encouraged to attempt to establish a secure connection from another device in order to verify that the same warning is shown and contact the remote service if the error persists. Further, participants are informed to never downgrade the HTTPS protocol to HTTP as this would remove the encryption.

Further Hints on the Attack. In order to be able to detect relevant encryption related browser warnings, participants are presented

with screenshots and explanations pertaining to all major current browsers.

A.2.7 Attack: Targeted guessing.

Description of Attack. In this approach attackers attempt to gain access to one specific user account by attempting to authenticate using likely passwords associated with the user. Sources for such passwords are for example social media or other public sources of information, such as company websites.

Description of Defences. Participants are encouraged to select passwords which cannot be associated with their person, by not incorporating information about them which is publicly available. When passwords are supposed to protect against spouses or close acquaintances, user are advised to consider what the respective person could deduce as password guess.

A.2.8 Attack: Untargetted guessing.

Description of Attack. In untargeted guessing scenarios, attackers attempt to obtain credentials for many user accounts at one specific service in parallel, i.e. trawling attacks [6]. Frequently used passwords (such as keyboard walks), passwords from past breaches, and dictionary words of a variety of languages are used as guesses for all known user accounts at the service under attack. This attack requires knowledge of valid usernames for the service, which are often publicly accessible (e.g. on sites where users post content, such as online forums) or available for purchase on the black market (e.g. for email services).

Description of Defences. This attack can be prevented by choosing infrequently used passwords, which also are not related to the service they are used for.

A.2.9 Attack: Guessing after a break-in.

Description of Attack. In this attack scenario an attacker has already compromised a service and obtained the stored credentials. If the credentials are stored as hashes usually a combination of brute-force and dictionary attacks are used in this case.

Description of Defences. Defence against this attack is two-part. First, service operators need to observe security best-practices, otherwise, all user efforts are in vain [11]. Second, participants are encouraged to select long passwords, especially for device login, password manager master-passwords, email account passwords, and single-sign-on passwords.

Further Hints on the Attack. Re-using passwords for multiple services increases the likelihoods of success of this attack.

A.2.10 Attack: Theft of unencrypted digital password notes.

Description of Attack. This attack targets credentials stored unencrypted on systems, physical media or in the cloud.

Description of Defences. The user is encouraged to store passwords only encrypted, i.e. to use a password manager, in particular when passwords are synchronised between multiple devices. If sharing a password is required in an emergency, transmission of the encrypted password should occur via encrypted channels if possible. Then, after the emergency-use of the password is finished, the password should be changed.

Further Hints on the Attack. Passwords which are sent to the user unencrypted, e.g. as replacement during a password reset, should be changed as soon as possible.

A.2.11 Attack: Exploiting a weak reset mechanism.

Description of Attack. This attack attempts to exploit week password reset mechanisms, allowing an attacker to change an account's password to a password known to him or her. This attack allows attackers to bypass even strong passwords.

Description of Defences. Defence against this attack depends on the type of password reset mechanism employed by the service. If password reset is based on the user's email address, a secure password for the email account must be ensured. If security questions are used as reset mechanism, it must be ensured that the answers to the security questions cannot be guessed. One possible solution is to treat the answers to security questions as passwords and store them in a password manager.

A.3 Technologies to Protect User Credentials

In order to mitigate the attacks described in the previous section, multiple technologies are available to users. For each introduced technology, first a general description is provided. Then, advantages and disadvantages of the technology are listed. Last but not least, where available, additional hints are provided to the participant.

A.3.1 Technology: Fingerprint Readers.

Description of the Technology. Fingerprint readers can be used to replace regular passwords with a biometric feature.

Advantages and disadvantages of the technology. On the one hand, using fingerprint readers is faster than entering passwords and also prevents shoulder surfing. On the other hand, photos or fingerprints taken from touched surfaces might be used to copy fingerprints. Further, changing ones fingerprints is not possible, if they are compromised.

Hints for using fingerprint readers. Fingerprint readers are readily available in a large variety of new consumer products. Some implementations can be used to replace large sets of different types of passwords (e.g. when the fingerprint is used to unlock a password manager or system keychain). Other biometric sensors in consumer products, such as face detection, might not be as mature and therefore not as secure.

A.3.2 Technology: Graphical Passwords.

Description of the Technology. Graphical passwords are used to replace text passwords or PINs and consist of graphical information. Examples include the Android pattern lock or the graphical password of the Windows operating system. Graphical passwords do not change the security level when compared to text passwords.

Advantages and disadvantages of the technology. Graphical passwords can be easier remembered by humans, however entry may

take longer allowing attackers more time to observe the entry. Furthermore, graphical passwords are incompatible with password managers.

Hints for using graphical passwords. If services allow for the use of graphical passwords, they usually can be used in conjunction with traditional text passwords. Similarly to text passwords, it is also possible to choose weak graphical passwords. Examples include symmetric patterns or clickable locations which are faces of persons, red items or corners and centres of items.

A.3.3 Technology: Hardware Tokens.

Description of the Technology. Hardware tokens can replace text passwords as authentication mechanisms. Examples for hardware tokens include USB devices, smartwatches and special chip cards.

Advantages and disadvantages of the technology. Hardware tokens prevent shoulder surfing and increase the difficulty of guessing attacks. However, if the token is stolen, the thief can authenticate using the token.

Hints for using hardware tokens. In the business context, the integration of hardware tokens should be coordinated with the IT department. Many hardware tokens can also be used as part of two factor authentication.

A.3.4 Technology: Password Manager.

Description of the Technology. Password managers support users in creating and storing secure passwords. They are available for many mobile and desktop platforms, some allow the synchronisation between different devices. Many security professionals use password managers, as they are an effective tool to prevent many of the attacks explained earlier.

Advantages and disadvantages of the technology. Password managers create secure, long passwords defending against guessing attacks. The use of browser plugins which allow auto-fill of passwords on websites for which passwords were previously stored, prevent phishing and shoulder surfing attacks. In most cases the secure usage of a password manager requires a strong master-password. If the master-password is lost, access to the stored passwords may become impossible.

Hints for using password managers. Selection of a password manager should consider the users requirements, for example if a browser plugin is required. Users should select a password manager which can also generate secure passwords. Secure master passwords should be selected, for example by concatenating multiple words. Weak legacy passwords (i.e. not generated using the password manager) should be replaced with stronger passwords when added to the password manager. New passwords for services should be created using the password managers password generator functionality.

A.3.5 Technology: Privacy filters.

Description of the Technology. Privacy filters can be used to prevent shoulder surfing by restricting the viewable angle of screens. This reduces the risk posed by observers behind or next to the user, for example while travelling via train.

Advantages and disadvantages of the technology. Privacy filters reduce the risk of shoulder surfing, however they may reduce the brightness of screens and the sensitivity of touch input.

Hints for using privacy filters. Depending on the user's device, different types of privacy filter may be required. In enterprise environments the use of privacy filters should be coordinated with the IT department.

A.3.6 Technology: Single-Sign-On.

Description of the Technology. Single-sign-on technologies allow users to authenticate to one service, which in turn confirms the identity and authenticity of the user to other services. This technology is common in enterprise environments but also available in private settings. If single-sign-on is used, the selection of a strong password for the identity provider is especially important.

Advantages and disadvantages of the technology. Single-sign-on solutions reduce the number of passwords and authentications required. Furthermore, single-sign on allows sharing of data associated to user accounts between the single-sign-on service and other services (and it thus does not have to be entered on each service individually, saving time during registration). As the other services require no password, guessing attacks and password attacks are not possible. However, the single-sign-on service is able to store information about services used by the user which might incur privacy issues. Additionally, the single-sign-on service represents a remote single point of failure. If the single-sign-on service experiences an outage, no authentication to the associated services is possible. If it is compromised, all accounts connected to the single-sign-on service are compromised as well.

Hints for using single-sign-on. The user is provided with an example of setting up a single-sign-on authentication using as example a popular webservice.

A.3.7 Technology: Two-factor authentication.

Description of the Technology. Two-factor authentication requires authentication using different factors, such as *something you know*, *something you are* or *something you have*.

Advantages and disadvantages of the technology. Two-factor authentication ensures that an attacker cannot access an account even if the users password is compromised, increasing the security level significantly. Two-factor authentication is recommended as an easy way to increase the security of important accounts such as the primary email address to which password reset emails are delivered. However, if two-factor authentication is used, all factors are required in order to authenticate. If the second factor is lost, restoring access requires more effort than a traditional password reset.

Hints for using two-factor authentication. Today, many services allow users to enable two-factor authentication. If different types of factors are available, the use of SMS authentication should be avoided [13].

Table 2: APPENDIX B: This table lists all scenarios used in the study. Since we conducted our study in Germany, the scenarios were originally developed and used in German and translated for this publication. For each attack there are two scenarios, one representing secure behaviour and one representing insecure behaviour.

Attack		#	Scenario
Fraudulent messages	Secure	1	Mr. Schmidt works together with his colleague Müller on the same project. Mr. Schmidt is the vacation substitution for his colleague. He receives an email in which his colleague asks him to send the project plan to his private email address, because he wants to work on it in his rainy vacation. Mr. Schmidt does not send the information to the private email address.
	Insecure	2	Mr. Schmidt's boss is on a business trip to visit a client. Mr. Schmidt receives an email in which his boss informs him that a person from the help desk of the client will contact Mr. Schmidt to get access to the web-interface of the project management software. Shortly after, Mr. Schmidt's phone rings: it is the person from the help desk. Since he received the announcement of the call from the email-address of his boss, Mr. Schmidt gives the person from the help desk the required password.
Theft of an insecurely stored note of the password	Secure	3	Mr. Schmidt finds it difficult to remember his passwords. Therefore, he keeps a note of his private passwords at home in a locked drawer of his desk, which only he can open.
	Insecure	4	Mr. Schmidt has to change the password for one system in the company every 90 days. He already had to call the help desk of his company multiple times to have them reset a pass-word he could not remember after a mandatory change. When changing the password for the next time, he makes a note of it and stores the note under his mousepad on his desk.
Shoulder-surfing	Secure	5	Mr. Schmidt sits in the train on his way to a client. The train is fully booked, the seat next to him taken. Mr. Schmidt checks emails using his smartphone. Due to an urgent request from his boss, he has to access the web-interface of the project management software used in this company to list a cost report. He notices that the person in the seat next to him tries to look at the screen of his smartphone inconspicuously. Therefore, he leaves his seat and moves to an area in the train where he is undisturbed, so that no one can spy on the sensitive data he is accessing.
	Insecure	6	Mr. Schmidt is sitting in a café and waits on his colleague to have lunch together. Since his colleague sent him a text message saying that he will be 30 minutes late, Mr. Schmidt wants to use the time to work on his laptop. While he is working a couple approaches and asks whether they can join him at the table. Since all other tables in the café are fully occupied, Mr. Schmidt agrees. One of them sits down on the opposing side of the table, one sits down next to Mr. Schmidt who continues his work and logs in multiple times to the web-interface of the project management software of his company.
Compromising the users' devices	Secure	7	Mr. Schmidt sits in his office. He is printing presentation slides for a meeting. The printer is located at the other end of the corridor. Before Mr. Schmidt leaves his desk to fetch the print-out, he locks his laptop.
	Insecure	8	Mr. Schmidt has to share a file with this colleague Mr. Müller. The file is too large to attach it to an email. Since he has no USB stick at hand, he uses the one he found last week in the parking lot of his company.
Eavesdropping on unencrypted communication	Secure	9	Mr. Schmidt is on his way to a client. Unfortunately, the train is delayed. Therefore, he sits down in a café at the train station. There he uses an open wifi. He uses his laptop as usual, but pays attention that he visits all websites using an encrypted connection.
	Insecure	10	Mr. Schmidt is on a business trip visiting a client in a different city. There he stays in a hotel and uses its charged premium unencrypted wifi to work in his room. To login to the wifi, he has to enter a user name and a password.
Eavesdropping on encrypted communication	Secure	11	Mr. Schmidt has to access the web-interface of a client's system. He receives a warning that no encrypted connection is possible although this has worked in the past. Therefore, Mr. Schmidt calls the client using a phone number known to him, describing the problem. He does not access the web-interface until the problem is solved.
	Insecure	12	Mr. Schmidt is at a client in a different city to prepare a new project. He has to stay several nights and books a room in a hotel. Once he is in his room, he tries to access the web-interface of the project management software of his company. He receives a warning stating there is problem with the security of the connection, although the connection is encrypted. The problem does not occur with the web-interface of his email account. He infers that the web-interface of the project management software is misconfigured and enters his credentials.

Continued on next page

Table 2 – *continued from previous page*

Attack		#	Scenario
Targeted guessing	Secure	13	Mr. Schmidt takes his private smartphone to work (but does not use it for business purposes). He does not want that friends or colleagues can access the phone by guessing his PIN. Since he shares the phone with his wife in their free-time, she should be able to easily re-member the PIN. Therefore Mr. Schmidt uses as PIN the birthday of the family dog, which is only known to him and his wife.
	Insecure	14	Mr. Schmidt finds it difficult to remember passwords. Therefore, he uses as password for his laptop at work *Alexander1997*, the first name and the year of birth of his child.
Untargeted guessing	Secure	15	Mr. Schmidt has to perform small design tasks. For this purpose, he has to open an account with Adobe to purchase and download software such as Photoshop and InDesign. For the user account, he chooses a long password (substantially longer than 8 characters), which is neither in the lists of frequently chosen passwords nor derived from the company name Adobe.
	Insecure	16	Mr. Schmidt has problems remembering all the passwords he needs for his job and privately. Therefore, he uses walks on the keyboard, such as *1q2w3e4r%*, to create secure passwords.
Guessing after a break-in	Secure	17	Mr. Schmidt is frequently on business trips and once he had his laptop almost stolen at the airport. Therefore, he encrypts its hard drive and chooses to encrypt the hard drive and to login a password with more than 20 characters which he creates concatenating multiple words to one another.
	Insecure	18	The company in which Mr. Schmidt is employed uses an external web service to store important client data. Mr. Schmidt learns that this web service was the target of a successful hacker attack and that password data was stolen. His password is *Al3xand3r!*, derived from the name of his son. Since the password is longer than 8 characters and contains multiple numbers and a symbol he does not change it.
Theft of an unencrypted digital note of the password	Secure	19	Since Mr. Schmidt has problems remembering the many passwords he needs for his job, he asks the it-department whether they can install a password manager on his work laptop. Since he wants to synchronise the passwords to his business smartphone, he chooses a master password with more than 20 characters, which he creates by concatenating multiple words.
	Insecure	20	Mr. Schmidt has to use many passwords in his daily job to log on to all the different systems needs to access. Since he also works on his business smartphone, Mr. Schmidt saves all the passwords in a Word document and synchronises this document through a public third-party cloud storage provider between his laptop and his smartphone.
Exploiting a weak reset-mechanism	Secure	21	Mr. Schmidt uses different external web services, as is usual in his company. For one of the web services, the password can be reset using personal security questions. Instead of answering the questions truthfully, Mr. Schmidt chooses a random character sequence as answers, writes this sequence down, and stores it where only he can access it.
	Insecure	22	Mr. Schmidt uses different web services in his private life. For one of the web services the password can be reset using a link in an email sent to him. As password for the respective email account he chooses *@lex@nder1997* (derived from the first name and year of birth of his son), since it is more than 8 characters long and contains multiple special characters.