View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by KITopen

Addressing Misconceptions About Password Security Effectively

Peter Mayer
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
peter.mayer@secuso.org

Melanie Volkamer
SECUSO - Security, Usability, Society
Technische Universität Darmstadt
Privacy and Security Research Group
Karlstad University
melanie.volkamer@secuso.org

ABSTRACT

Nowadays, most users need more passwords than they can handle. Consequently, users have developed a multitude of strategies to cope with this situation. Some of these coping strategies are based on misconceptions about password security. In such cases, the users are unaware of their insecure password practices. Addressing the misconceptions is vital in order to decrease insecure coping strategies. We conducted a systematic literature review with the goal to provide an overview of the misconceptions about password security. Our literature review revealed that misconceptions exist in basically all aspects of password security. Furthermore, we developed interventions to address these misconceptions. Then, we evaluated the interventions' effectiveness in decreasing the misconceptions at three small and medium sized enterprises (SME). Our results show that the interventions decrease the overall prevalence of misconceptions significantly in the participating employees.

CCS CONCEPTS

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

KEYWORDS

password security, misconceptions, literature review, user study

ACM Reference format:
Peter Mayer and Melanie Volkamer. 2017. Addressing Misconceptions About Password Security Effectively. In *Proceedings of 7th Workshop on Socio-Technical Aspects in Security and Trust, Orlando, Florida, USA, December 2017 (STAST 2017),* 12 pages.
https://doi.org/10.1145/3167996.3167998

1 INTRODUCTION

Text passwords are ubiquitously used to authenticate users, be it online or offline. Yet, many users face problems when choosing, handling, or remembering their text passwords [15, 16, 28]. As a result, users have developed a variety of coping strategies. Some of these coping strategies can be beneficial, e.g. using a master-password protected password manager in order to cope with remembering different passwords for all accounts. However, some of these coping strategies are based on misconceptions about password security, e.g. a misconception about what exactly makes a password hard to guess for attackers might lead users to add a '!' to end of the password to make it secure [18]. This leads to situations, where users believe that they have secure password practices, when in reality they do not: the users are simply unaware of their insecure password practices.

Misconceptions about password security appear frequently in published literature, e.g. the lack of mental models representing automated attacks and defenses against them [18]. Knowing the prevalent misconceptions and addressing them with effective interventions is vital, when aiming to decrease insecure coping strategies. Thus, the overall aim of this work is to identify and address the misconceptions about password security reported in the literature.

To realize this work, we applied the four step process depicted in Figure 1. First, we conducted a systematic literature review to identify the misconceptions about password security reported in the literature (step 1). Therein, we identified 23 different misconceptions about password security. We found that there exist misconceptions in basically all aspects of password security and that four categories of misconceptions emerged. Additionally, we found that only some of the misconceptions always apply, while others depend on the particular situation the user is confronted with.

Then, we developed interventions to address the misconceptions identified in our literature review (step 2). The development included refinements derived from structured expert feedback. Using the developed interventions, we then conducted a formal user study (step 3) to evaluate the interventions' effectiveness with overall 90 employees in three small and medium-sized enterprises (SME). We find that our interventions significantly decrease the overall prevalence of the identified misconceptions. Last but not least, we propose further refinements for the interventions (step 4), based on the results of the user study.

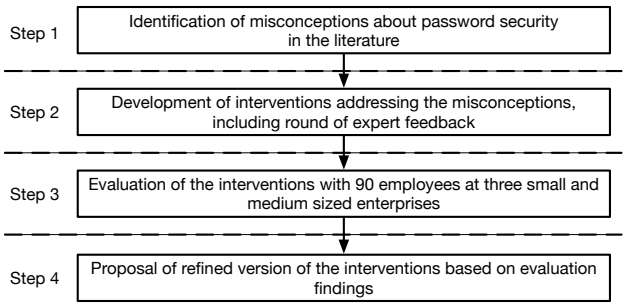

Figure 1: The process underlying this work.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
STAST 2017, December 2017, Orlando, Florida, USA
© 2017 ACM.
ACM ISBN 978-1-4503-6357-0/17/12…$15.00
https://doi.org/10.1145/3167996.3167998

The core contributions of this work are:

(a) Providing a list of the misconceptions about password security reported in the literature.
(b) Providing formally evaluated interventions which address the identified misconceptions and decrease their overall prevalence.

The remainder of this work is structured as follows. In the next section (section 2), we present and discuss the methodology as well as the results of our literature review. Then, we describe the development of our interventions (section 3). Thereafter, we present the methodology as well as the results of our user study and discuss both (section 4). Lastly, we conclude and point out areas for future work in section 5.

2 LITERATURE REVIEW

In this section we present the methodology and results with respect to our first contribution, the identification of misconceptions about password security in the published literature.

2.1 Methodology

We conducted a systematic literature review to identify all the misconceptions regarding password security reported in the literature. Since the goal of this research is to give an up-to-date overview of misconceptions about password security, we only considered publications from the last decade, i.e. published since 2007. After consultation with native English speaking experts in the field, we used as search terms "password" in conjunction with each of the terms "misconception", "misunderstanding", "misperception", "flawed perception", and "flawed understanding", one after the other. Both terms (i.e. "password" and any one of the other search terms respectively) needed to be present in the publication. As sources for the publications, we relied on (a) the databases Sciencedirect, ACM, IEEExplore, SpringerLink, and Scopus, as well as (b) additional conferences and journals known to publish relevant research on passwords, but not indexed by the used databases, i.e. Usenix Security Symposium, Symposium On Usable Privacy and Security, Usable Security Workshop, Trustworthy Interfaces for Passwords and Personal Information Workshop, Journal of Computer Security, International Journal of Information Security and Privacy, International Journal of Technology and Human Interaction, Human IT: Journal of information technology studies as a human science, MIS Quarterly, Journal of Information Systems Security. We found 3777 publications meeting the search terms in the sources.

From the 3777 publications meeting the search terms, we narrowed down the body of relevant literature. Publications not accessible through the authors' universities' libraries were excluded. For publications where the respective authors had published the same results multiple times (e.g. extended versions of conference papers in journals), only the latest publication was considered. Also, non-peer-reviewed publications (white-papers, technical reports, etc.) were excluded. To filter out the publications not explicitly dealing with misconceptions in field of passwords, the publications were manually screened based on title, abstract and if necessary a glance on the full text. 15 relevant publications reporting on misconceptions met these additional search criteria. To broaden the results, first a forward, then a backward search was performed, resulting in overall 20 relevant publications. The full list of relevant publications identified in our literature research can be found in section 7.

2.2 Results

Based on these 20 relevant publications, we identified 23 misconceptions about password security. In the following, we describe each of the identified misconceptions. Note that we list all misconceptions reported in the literature, even when there is no sharp definition in the respective publication. Also, some of the misconceptions are not universal, i.e. they only apply in certain attack scenarios. A through discussion is beyond the scope of this work, but this aspect will be briefly discussed in the following where necessary.

2.2.1 The inclusion of numbers makes passwords automatically more secure. M1 was reported in five publications: [1, 12, 14, 17, 18]. The underlying problem with this misconception is that additional character classes (i.e. lowercase, uppercase, numbers, symbols) can make passwords more secure, but this is not automatically the case. Research has shown that (a) when users try to add additional character classes to their passwords, they tend to create very predictable passwords [17] and that (b) forcing users to put these characters in places where they contribute most to the guessing-resistance of the passwords decreases the usability of the created passwords [14]. This misconception can be assumed to be universal, since it applies to all attack scenarios where passwords are guessed.

2.2.2 The inclusion of symbols makes passwords automatically more secure. M2 was also reported in five publications: [1, 12, 14, 17, 18]. The underlying problem is the same as for M1: users tend to put the chosen symbols in predictable places in the password. Analogously to M1, this misconception should also be assumed to be universal.

2.2.3 The inclusion of uppercase letters makes passwords automatically more secure. M3 was reported in two publications: [1, 17]. The underlying problem is the same as for M1and M2: users tend to put the uppercase letters in predictable places in the password (in particular in the front). Analogously to M1 and M2, this misconception should also be assumed to be universal.

2.2.4 Common substitutions (e.g. a → 4) make passwords more secure. M4 was reported in two publications: [17, 19]. The underlying problem is the same as for M1, M2, and M3: users tend to use predictable substitutions in efforts to make their passwords more secure. Analogously to M1, M2, and M3, this misconception should also be assumed to be universal.

2.2.5 A word from another language than the user's mother tongue is a secure password. M5 could be identified in one publication: [16]. The underlying problem with this misconception is that attackers can easily build large dictionaries with words from several languages using e.g. the freely available wikipedia entries in nearly 300 languages. However, this implies that the attacker has a large number of guesses available which is usually only the case in offline attacks. Consequently, this misconception mostly relevant to offline attack scenarios.

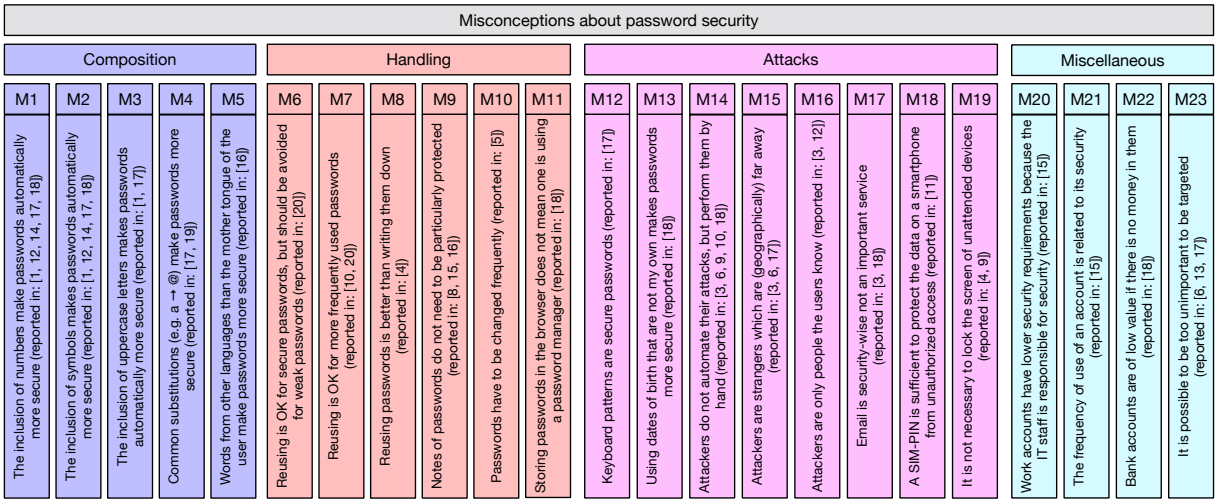

Figure 2: Overview of all misconceptions about password security identified in the literature review.

2.2.6 Reusing passwords is OK for secure passwords, but should be avoided for weak passwords. M6 is one of three misconceptions concerning the reuse of passwords, which is a common coping strategy of users [34]. It was reported in one publication: [20]. The underlying problem with this misconception is that users applying this misconception in their handling of passwords might end up with secure passwords at more websites, but at the same time increase the risk of cross-site attacks [20] (e.g. when a website leaks passwords in the clear and that password is used by an attacker to break into an account at another website). In particular, this misconception does not include the real metric on which a decision to reuse a password should be based: whether reusing a password would allow an attacker to compromise additional valuable data [25, 29]. This misconception applies to all attack scenarios, where users have accounts at multiple websites. Thus, it can be assumed to be true for most users today.

2.2.7 Reusing passwords is OK for passwords that are entered more frequently. M7 could be identified in two publications: [10, 20]. The problem underlying this misconception is the same as with M6: it does not include the real metric on which a decision to reuse a password should be made. Thus, users might reuse passwords across accounts that give access to different valuable data. Analogously to M6, this misconception applies to all attack scenarios, where users have accounts on multiple sites.

2.2.8 Reusing passwords is more secure behavior than writing them down. M8 was identified in one publication [4]. The underlying problem of this misconception is that while users can control where they store written down passwords (i.e. they can make sure it is stored securely), they have no way of knowing whether a web service is among the many not sufficiently protecting the users' data [22] (i.e. their password might be insecurely stored, without the users having any way of knowing). Analogously to M6 and M7, this misconception applies to all attack scenarios, where users have accounts on multiple sites.

2.2.9 Notes of passwords do not need to be particularly protected. M9 regards the handling of paper notes as well as electronic notes [15]. It was reported in three publications: [8, 15, 16]. The problem underlying this misconception is that notes of passwords can be beneficial and have been recommended by security experts (e.g. [33]), but this advice always comes with the condition of secure storage of that note. Thereby, in particular the unprotected storage of cleartext passwords in the cloud (e.g. a text document in Dropbox or in note-taking services such as OneNote) poses a severe risk. This misconception applies to all attack scenarios, where an attacker might get access to a note of a password. With respect to physical notes this includes physical access to the place where it is stored. When electronic notes are stored in the cloud, the variety of attack scenarios is much larger and potentially includes e.g. rogue administrative staff at cloud services or unencrypted transfer of the password data in the clear to the cloud service.

2.2.10 Passwords have to be changed proactively on a regular basis. M10 was reported in one publication: [5]. The problem underlying this misconception is that research [24, 38] indicates that changing passwords on a regular basis does not improve practical security and instead only puts unnecessary burden on the user. As a matter of fact, while it was still included in earlier versions, the-most recent versions of password advice from the US NIST [26] and the British NCSC [29] both discourage using mandatory password changes, unless a user account has actually been compromised. This bares potential for confusion among users, since not all standardizing bodies have adapted their standards with respect to these findings (e.g. PCI-DSS [31]). With respect to the relevant attack scenarios, this misconception is universal, since it potentially applies to all of the user's passwords.

2.2.11 Storing passwords in the browser does not mean one is using a password manager. M11 indicates that users mistake technologies that are essentially the same as different. It was reported in one publication: [18]. The underlying problem of this misconception is that users on the one hand argue that using dedicated

password managers is insecure, but on the other hand store their passwords in browsers. It is important that users understand that the same security requirements (e.g. setting a master-password in most situations) apply to dedicated password managers and those integrated in browsers. This misconception is relevant in all attack scenarios, where an attacker could access the passwords which are stored in the browser (e.g. physical access to the device or storage disk).

2.2.12 Keyboard patterns are secure passwords. M12 was reported in one publication: [17]. The problem underlying M12 is that while patterns on the keyboard might seem like random passwords, the security issues associated with using them for passwords are well documented [17, 36]. This misconception applies to all attack scenarios where guessing attacks are viable and therefore should be considered to be universal.

2.2.13 Using dates of birth that are not the user's makes passwords more secure. M13 was reported in one publication: [18]. The security issues associated with using dates as passwords are well documented [37]. Analogously to M12, this misconception is relevant in all attack scenarios where guessing attacks are viable and can thus be assumed to be universal.

2.2.14 Attackers do not automate their attacks on passwords, but perform them by hand. M14 was reported in five publications: [3, 6, 9, 10, 18]. The underlying problem of this misconception is that users underestimate the scale of attacks that specialized tools allow. This misconception is relevant in all attack scenarios were automation is possible (e.g. phishing attacks [30]). Thus, it is not relevant in attack scenarios that are difficult to automate (e.g. attacks requiring physical access to the users' device).

2.2.15 All attackers are strangers which are (geographically) far away. M15 was found in three publications [3, 6, 17]. The problem underlying this misconception is that it limits the perception of possible attacks. However, there are many motives for an attack on a user's passwords or accounts, but not all of them relate to an unknown hacker which is geographically far away, e.g. someone impersonating cleaning personnel or help desk staff to get access to an office, co-workers who want that changes cannot be traced back to them, or a nosy acquaintance who wants to spy on the communication with other users. This misconception is universal, since it applies to potentially all passwords of a user.

2.2.16 All attackers are people the users know. M16 represents the opposite assumption of M15. It was reported in two publications: [3, 12]. The underlying problem of this misconception is the same as for M15: a disregard of likely attacks (e.g. trawling attacks, where attackers target as many accounts and the goal is not to get into one specific account, but in as many accounts as possible [21]). Analogously to M15, this misconception is universal.

2.2.17 Email is security-wise not an important service and therefore does not require a secure password. M17 was reported in two publications: [3, 18]. The underlying problem of this misconception is that insufficiently protected email accounts can compromise other accounts if passwords can be reset using links sent by mail. Thus, a compromise of the user's email account can cause a snowball effect of further compromises. Additionally, attackers can use compromised accounts to send out spam in the user's name. This misconception is relevant for all email accounts that are used by the user to communicate with others or that can be used to reset the passwords of other accounts.

2.2.18 A SIM-PIN is sufficient to protect the data on a smartphone from unauthorized access. M18 was identified in one publication: [11]. Its underlying problem is that only a system PIN used to lock a device protects the data on the respective device. A SIM-PIN can be easily circumvented by removing the SIM from the device. This misconception applies to all attack scenarios, where the user has cellular devices allowing removal of the SIM card.

2.2.19 It is not necessary to set a password to lock the screen of unattended devices. M19 was reported in two publications: [4, 9]. The underlying problem is that attacks aiming at physical access to the user's devices are neglected (e.g. impersonation of help desk staff or cleaning personnel). Analogously to M9, this misconception is relevant in all attack scenarios, where an attacker can gain physical access to a user's devices.

2.2.20 Work accounts have lower security requirements because the IT staff is responsible for security. M20 was identified in one publication: [15]. The problem underlying this misconception is that users might perceive their work account differently than their private accounts, while it is exposed to at least the same degree of threats. This misconception is relevant in all attack scenarios, where users have both, private and work accounts.

2.2.21 The frequency of use of an account influences its security requirements. M21 was reported in one publication: [15]. The underlying problem is that it disregards the aspects that actually influence the security requirements of an account (i.e. data accessible in the account and actions which can be performed with the account). This misconception should be assumed to be universal, since it potentially affects all accounts of a user.

2.2.22 Bank accounts do not need to be protected with strong passwords if there is no money in them. M22 was identified in one publication: [18]. The problem underlying this misconception is that while some research reports that financial sites are of high value to users (e.g. [15]), in others users voiced that if there was no money in their account, the security requirements would be low. Whether this misconception applies to a user depends on factors such as whether the account can be overdrawn and being left with debts (and the incurring interest) might be a concern. In contrast, if the account cannot be overdrawn, there is no money in it, and the attacker does not have any possibility to transfer any money from other accounts of the user to that particular account and then withdraw it, the security requirement might indeed be low.

2.2.23 It is possible to be too unimportant to be targeted and thus to have to choose secure passwords. M23 was reported in three publications: [6, 13, 17]. The underlying problem of this misconception is that not being aware of attacks as well as corresponding counter-measures renders users even more vulnerable to attacks. This misconception is universal with respect to the relevant attack scenarios, since it potentially affects all passwords of the user.

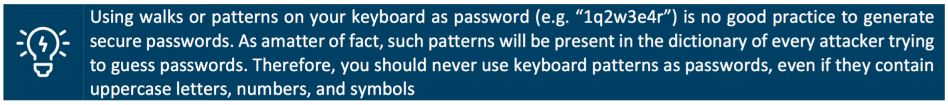

Figure 3: Example of the design of the interventions after the expert evaluation.

2.2.24 Further Findings. During our literature review, we encountered two further misconceptions, which will not be regarded in the remainder of this work. The first one states that security updates are not important (reported in [5]). It does not pertain to password security directly, but revolves around one advice deemed most important by security experts [5]: installing security updates. The second one concerns password managers. While using password managers is generally considered to be good advice [5, 16], there also exists a mistrust towards them (reported in [2, 5, 7]). Such a lack of trust is difficult to address with explanatory texts. One might try to convince users by explaining to users that experts in the field trust password managers (as e.g. found in [16]). Yet, trust is not easily established by textual communication [23, 32]. Therefore, this lack of trust should not be treated as an issue which can be addressed by knowledge transfer and will not be regarded in the remainder of this work. However, following up on this issue might be an interesting field for future investigations.

2.3 Discussion

Overall, we identified 23 misconceptions in the published literature. These span a wide variety of aspects, from the inclusion of different character classes to the security trade-offs between reuse and writing passwords down. Thereby, four broader categories of misconceptions emerged: composition, handling, attacks, and miscellaneous. Figure 2 depicts all the misconceptions we identified along those five categories.

Composition: This category comprises all misconceptions regarding the password composition, such as inclusion of different character classes (i.e. letters, numbers, and symbols) by the user.

Handling: This category includes all misconceptions with respect to behaviour associated with the handling of passwords, such as reuse of passwords for multiple accounts.

Attacks: This category contains all the misconceptions concerning the attackers and their strategies, that do not directly relate to password composition or the handling of passwords.

Miscellaneous: This category consists of further, more general, misconceptions, which were found in the literature to also apply to password security as well.

Note that certain limitations apply to our work, as is the case with every systematic literature review. We explicitly excluded non-peer-reviewed publications and those published before 2007. This might have limited our results and led to the exclusion of relevant work. However, we argue that in both cases the exclusion generally increases the quality and relevancy of the literature included in our systematic literature review: non-peer-reviewed publications might introduce low quality results and too old publications might lead to the inclusion of misconceptions which are not relevant anymore.

Lastly, a broader selection of search terms might have resulted in more relevant research. Yet, we argue that our process of screening literature and feedback from native English speaking experts in the field, represents the most systematic way to choose appropriate search terms for the literature review.

3 DEVELOPMENT OF THE INTERVENTIONS

To address the misconceptions we identified in our systematic literature review, we developed interventions for each of them. We decided to develop a text based intervention, since this allows supporting multiple training formats (e.g. instructor-based, computer-based or text-based as proposed in [35]).

As a first version of the interventions, we created short texts for each of the misconceptions, which explained the misconception itself, the scenarios it is relevant in, and the respective underlying problem (e.g. the underlying problem with M1 is that numbers only improve the guessing resistance of a password, if they are put in an unpredictable place in the password). The wording and contents of this first version of the interventions were iteratively improved using informal feedback from information security and psychology experts as well as lay users. During this iterative design, it became clear that in three instances the interventions of multiple misconceptions converged to very similar texts and only differed slightly in the wording. On multiple occasions throughout the development, we received feedback that these misconceptions might be better addressed together. Therefore, we integrated the texts of multiple misconceptions into one in these three instances: (1) M1, M2, M3, and M4, (2) M6 and M7, and (3) M15 and M16.

To improve this first version, we held a round of structured expert feedback with the goal of collecting additional opinions regarding the interventions' texts and expert assessments of whether the identified misconceptions had been overall sufficiently addressed from an information security point of view. For this purpose, we created a PDF-file with all interventions and a free text field for each intervention, in which the experts could enter their feedback.

We contacted 30 independent information security experts from academia and from the industry (i.e. researchers, information security consultants, auditors, and administrative staff) and sent them the interventions with instructions to give feedback for each individual intervention. From the 30 experts we sent invitations to, 13 sent us their feedback. We received responses from three scientists, 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 developing security solutions. Thus, we received feedback from a diverse set of experts.

The expert feedback round lead to several refinements of the interventions, such as additional explanations in the texts, e.g. concerning M19 the experts suggested adding more concrete information about possible attackers: "*The following types of people should be included as potentially interested in the users data: Cleaning personnel, nosy co-workers, or future ex-co-workers.*" (Expert 7) or "*Explanations with respect to who might try to access the devices should be added [for example], cleaning personnel [or] nosy colleagues.*" (Expert

Table 1: The wording of the intervention texts after the round of expert feedback. Note that the wording represents a translation into English from the German original versions created for the study. Creating German texts was necessary to allow the study presented in Section 4.

ID	Wording of the Intervention after Expert Feedback
M1	Using specialized software, attackers try to mimick human behaviour when guessing passwords. Thereby, they use a long list of words (from dictionaries, but also passwords from past breaches) and apply different common modifications to these words to generate additional words they will also use as guesses for the password: • Appending or prepending numbers and symbols (e.g. adding an "!" to the end is a popular choice) • Substituting letters with numbers (e.g. E → 3) or with symbols (e.g. a → @) • Substituting lowercase letters with uppercase letters (in particular at the beginning of words) Therefore, using numbers, symbols, or uppercase letters in your password will not automatically make it harder to guess.
M2	
M3	
M4	
M5	While it might seem that using a word from a language that is not your mother tongue as password is secure, this can be very problematic. In particular when attackers can make a large number of guesses for each account (e.g. there is no limit on the login attempts at a web service), they will use words from many languages to try and guess your password.
M6	Unfortunately, it happens time and again that even large web services handle the passwords of their users carelessly which then leak to attackers. Therefore, even passwords which are very hard to guess should not be reused. If a password is leaked by a service in the clear, it does not matter how hard it is to guess. This also holds for passwords you enter frequently. Do not reuse them. The more often you reuse a password at different services, the bigger is the chance of it getting into the hands of an attacker.
M7	
M8	If you store a written down password in a safe and secure location, making such notes can actually be beneficial (e.g. after changing a password until you have memorized it). However, if you do not need a note of a password anymore, you should dispose it (e.g. burn it). If you keep your written down passwords securely stored, having such notes is more secure than reusing passwords: Guessing a unique password is more difficult to guess than a password that might have leaked from another service which was affected by a leak, even if that password is a variation of a different password.
M9	Written down passwords must always be stored in a secure location (i.e. a location that can only be accessed by yourself). If you use a password manager you should in most cases set a strong master password. Only in cases where all of the four criteria below are met, it is not mandatory to set a password: • You are the only user of your devices • The hard drive of your device is encrypted • You do not synchronize your passwords across your devices • You always lock your devices, when you are not using them
M10	Scientists have found that changing passwords you need to remember proactively (i.e. without occurrence of an incident) is unhelpful in protecting your accounts. The additional effort required of the users is unproportionally larger than the achieved security benefits. Even governmental bodies, such as the US NIST or the British NCSC are already adapting their recommendations. They recommend to change passwords only when the old one has fallen into the hands of an attacker instead of changing it proactively. These governmental bodies believe that the web services have to implement a rigorous monitoring of their own systems and that they should use so-called lock-out mechanisms (e.g. limiting the number of possible login attempts). Changing passwords that have to be remembered is therefore obsolete advice which should not be followed anymore.
M11	Internet browsers often have an integrated password manager, which allows saving passwords entered on websites. Saving passwords in a browser is the same as saving them in a dedicated password manager. If the hard drive of your device is not encrypted and your passwords are saved in a password manager, which is not protected by a master password (no matter if in a browser or as dedicated program), attackers can easily copy your passwords off your hard drive, if they have physical access to it or your device is infected with malware.
M12	Using walks or patterns on your keyboard as password (e.g. "1q2w3e4r") is no good practice to generate secure passwords. As a matter of fact, such patterns will be present in the dictionary of every attacker trying to guess passwords. Therefore, you should never use keyboard patterns as passwords, even if they contain uppercase letters, numbers, and symbols.
M13	Attackers can easily use specialized software to guess all combinations of days, months, and years. Therefore, using your dog's birthday or the birthday of your favorite actor instead of your own will not render your password harder to guess for a professional attacker. This holds in all situations, where attackers can make large numbers of guesses (e.g. when a web service does not limit the number of possible login attempts, before the account is locked).
M14	Attackers can easily automate their attacks using readily available specialized software. Using such software, attackers can easily e.g. test many different passwords or snoop on unencrypted network traffic.
M15	Some people think that only cyber-criminals from the other side of the planet will typically attack them. Others believe that only those close to them will try to get access to their devices. However, attackers can come from both of these groups (and anywhere in between), e.g. a criminal hacker trying to access your bank account, a person posing as a co-worker, a co-worker trying to hide illegitimate access to sensitive information and framing others, a jealous friend who wants to check your communication with others, or a criminal employee of a cloud service who uses his position and access to user data to gain illegitimate profit.
M16	

Continued on next page

Table 1 – *continued from previous page*

ID	Wording of the Intervention after Expert Feedback
M17	Even if you use your email account only to send messages to others, it is still a valuable target for attackers. Exploiting the possibility to reset passwords of other accounts is particularly relevant. Your email account holds email from all the services you use. Therefore, attackers can easily look up all the web services you use and reset their passwords to access them.
M18	The SIM-PIN is the PIN you have to enter to unlock the telephony functions of your mobile phone. This PIN is not sufficient to protect the data which is stored on a smartphone. An attacker with physical access to the phone can easily remove the SIM from the phone to bypass this check. Moreover, many phones simply allow bypassing the entry of the SIM-PIN, resulting in a phone that is not able to make calls, but is unlocked to access all data on it.
M19	You should set a password lock and use it whenever you leave a device unattended – even if a co-worker or friend is in the vicinity (e.g. same office). If during your absence these people leave too (e.g. are called away, make telephone calls, or go to the toilet) your device is completely unprotected. However, even when your co-workers remain in the vicinity of the device, an attacker disguising himself as cleaning personnel or a support technician might be able to access a device unnoticed.
M20	You are responsible for the security of your devices, even at work when there is a dedicated IT department. The staff of the IT department can help you, but in the end it is your job to keep the device secure. Most attacks on organizations target the employees first, in order to get access to internal systems.
M21	The value of your accounts is not influenced by how regularly you use it. Instead, the only determining factors are the data which can be accessed in the account and which actions can be performed in the account.
M22	Money is not the only valuable associated with your bank account. When accessing your online banking account, attackers can easily see where you are shopping, when you book your holidays and where you are paying abroad, your address, your phone number … All they need is your password, no TANs are needed. *(Note for readers: TANs are transaction numbers. All German banks require these to authorize transactions. Since all participants in our study were German, all knew this term and its semantics in the context of online banking.)*
M23	Some people believe that they are not important enough to even be targeted by attackers. This is a misjudgment which can have potentially severe consequences. Many attacks on the Internet (e.g. guessing passwords of users at a web service or sending phishing emails) can be easily automated and are then performed in an untargeted fashion. The attacker does not care who's account they can access, they just try to get access to as many accounts as possible. Especially getting access to your devices is always interesting for an attacker. Attackers have many uses for your devices, even if you believe there is no valuable data on them. They can encrypt all your files and demand a ransom to decrypt them again, they can install programs which run in the background that can be used to attack other users, or they can even make your device act as a server on the Internet to host a phishing or scamming website tricking other users.

2). The wording of all intervention texts after the expert feedback round can be found in Table 1.

Additionally, there was consistent feedback from the experts on the presentation of the misconceptions, i.e. that they should be visually separated to allow recognizing the texts as misconceptions even when integrated in longer texts on password security (e.g. "*I would recommend to introduce visual elements (e.g. boxes) to make the misconceptions stand out.*" (Expert 10)). We adapted the presentation of all misconceptions accordingly by adding a dedicated memorable icon and a colored box. This design was iterated using informal feedback from lay users. The final design is illustrated in Figure 3.

4 USER STUDY

The wording of the intervention texts after the expert feedback round was then evaluated with lay users in a user study. The goal of this user study was to evaluate the effectiveness of the intervention texts in eliminating the identified misconceptions. The respective hypotheses for our research are:

H_O: *The intervention significantly decreases the overall prevalence of the identified misconceptions.*

H_{Mx}: *The intervention for misconception Mx significantly decreases the prevalence of Mx.*

Thereby, H_O represents the overall hypothesis with additional hypotheses H_{Mx} for each of the misconceptions.

4.1 Methodology

The evaluation consisted of three phases: (a) a pre-treatment questionnaire measuring the prevalence of the different misconceptions in our participant sample, (b) the treatment using the version of the interventions after the expert feedback round alongside information describing attacks on passwords and user accounts as well as respective defences, and (c) a post-treatment questionnaire measuring the prevalence of the different misconceptions in our participant sample after having been exposed to the interventions as well as collecting basic demographics data. Consequentially, the user study employs a within-subject design. Every participant saw all interventions. The study methodology conforms to all requirements of our university's ethics commission.

Both, the pre-treatment and post-treatment questionnaires used the same statements as study items (see Table 2 in the appendix). For each of those items, the participant had to state whether they believe the statement was correct or incorrect. The order of the items was randomized for each participant for both, the pre-treatment and the post-treatment questionnaires. Note that 9 out of the 24 items are formulated as the inverse of the respective misconception, in order to give the participants both correct and incorrect statements

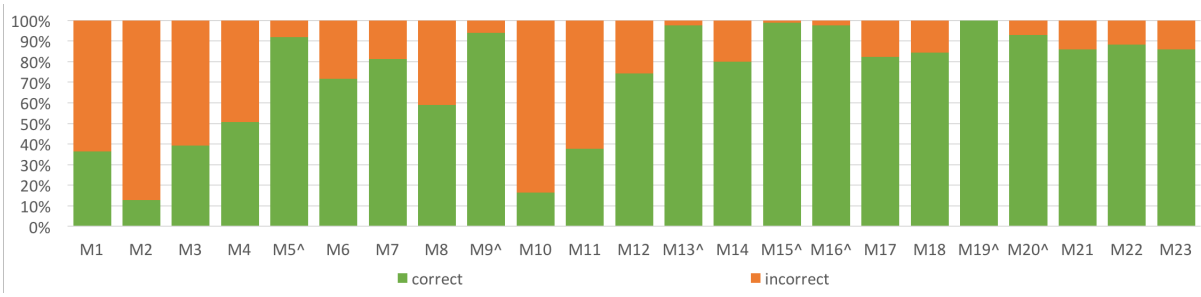

Figure 4: The correct and incorrect responses for each of the misconceptions *before* reading through the intervention texts. The misconceptions affected by ceiling effects are marked with a '^'.

to respond to. The items were developed in an iterative process using feedback from independent experts and from two rounds of pre-tests with lay users.

We decided to follow the recommendation by Haeussinger and Kranz [27] to evaluate materials for employees in real work environments employing experimental research designs. Therefore, the evaluation was conducted with employees at three small and medium-sized enterprises (SME). We conducted the user study in German SMEs and therefore both, the interventions 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 organizations. The recruitment in the organizations was done completely by the contact persons, who were given the instruction to select only lay people from their organization. The contact person also sent out and collected the PDF-files. Using a contact person as intermediary in each organization ensured that participants remained anonymous while being able to deliver the study materials to them via email in their real work environments. Participants received the questionnaires and the interventions as PDF-files one after the other as per the three phases outlined before (i.e. one PDF-file per phase). Only upon sending back the completed pre-treatment questionnaire to the contect person, the participant received the interventions with the instruction to take their time to read them. Once the participants confirmed that they had read the interventions, they received the post-treatment questionnaire. Once all participants in an organization had completed the post-treatment questionnaire, the contact person sent the filled out questionnaires to the authors.

4.2 Results

In this section, we present the results of our user study: first the demographics of the participants, then the results concerning the prevalence of the misconceptions identified in our literature review.

4.2.1 Participants. Overall 90 employees from three SMEs in Germany were recruited for our user study. Unfortunately, 6 participants had to be excluded from the analysis. 56 participants were male, 27 were female, one participant did not fill this question. The participants' age ranged from 19 years to 43 years (M: 30.0 years; SD: 5.4 years).

4.2.2 Analysis of the overall hypothesis. As becomes apparent from Figure 4, most of the misconceptions were prevalent in our sample of SME employees during the first phase of the study (i.e. before the treatment). Some of the misconceptions appeared in the majority of the participants. In particular, misconceptions M1, M2, M3, M4, M10, and M11 show low portions of correct responses and seem to be especially prevalent in our sample before the intervention. In contrast, some misconceptions are not prevalent in our sample. They can be identified by ceiling effects. A ceiling effect appears when the number of correct responses in the pre-treatment questionnaire is already so high that a significant increase of correct responses cannot occur, i.e. even if all incorrect responses in the pre-treatment questionnaire would be affected by the treatment and resulted in correct responses in the post-treatment questionnaire, this would not result in a significant difference. Such ceiling effects appear for the misconceptions M5, M9, M13, M15, M16, M19, and M20.

After the intervention, the overall portion of correct responses increases from 72.8% in the pre-treatment questionnaires to 90.2% in the post-treatment questionnaires. A Wilcoxon signed rank test with continuity correction shows a significantly higher number of correct responses per participant in the post-treatment questionnaire than in the pre-treatment questionnaire of the evaluation ($V = 58, p < .001$).

4.2.3 Analysis of individual misconceptions. Figure 5 shows for each misconception the individual differences in correct and incorrect responses between the pre-treatment questionnaire and the post-treatment questionnaire. We tested the individual differences with McNemar's test using Bonferroni-Holm corrected α-levels.

On the one hand, all of the misconceptions which stood out with high numbers of incorrect responses before the treatment show a significant improvement: M1 ($\chi^2(1) = 41.02, p < .001$), M2 ($\chi^2(1) = 28.27, p < .001$), M3 ($\chi^2(1) = 38.03, p < .001$), M4 ($\chi^2(1) = 39.02, p < .001$), M10 ($\chi^2(1) = 40.42, p < .001$), and M11 ($\chi^2(1) = 15.72, p < .001$). Yet, it is of note that despite showing a significant improvement, M2 still exhibits 48.9% incorrect answers in the post-treatment questionnaire. The misconceptions with higher numbers of correct pre-treatment responses showing significant improvements after the treatment are M6 ($\chi^2(1) = 15.43, p < .001$), M8 ($\chi^2(1) = 10.03, p = .002$), M18 ($\chi^2(1) = 11.08, p < .001$), and M23 ($\chi^2(1) = 9.09, p = .003$).

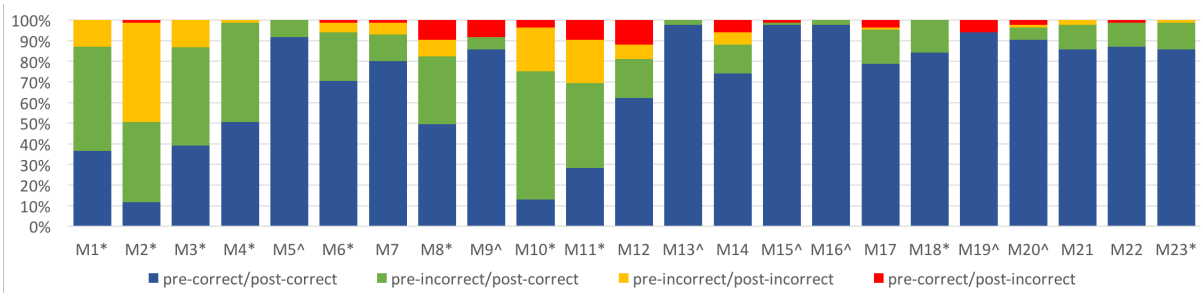

Figure 5: The correct and incorrect responses for each of the misconceptions before and after reading through the intervention. Each color represents the respective number of participants with "*pre-treatment*/*post-treatment*" responses, e.g. "pre-incorrect/post-correct" is the number of participants having responded incorrectly in the pre-treatment questionnaire and correctly in the post-treatment questionnaire. The misconceptions with significant improvements are marked with a '*'. The misconceptions affected by ceiling effects are marked with a '^'.

On the other hand, despite the decrease of the overall prevalence of misconceptions, the number of correct responses did not increase for all misconceptions from the pre-treatment questionnaire to the post-treatment questionnaire. Namely, the two misconceptions M9 and M19 exhibit more incorrect answers in the post-treatment questionnaire than in the pre-treatment questionnaire. However, for both the difference between pre-treatment questionnaire and post-treatment questionnaire we did not find significant differences.

For the remaining misconceptions where our analysis showed no significant difference in the correct answers between the pre-treatment questionnaire and the post-treatment questionnaire (i.e. M7, M12, M14, M17, M20, M21, and M22), there does not seem to be one unique reason. We will discuss possible reasons in section 4.3.

4.3 Discussion and Final Refinements

In this section, we discuss the findings of our user study and derive from them the proposals for refinements to the interventions where appropriate. Note that the empirical validation of these refinements is still furture work. We first discuss the overall findings and then discuss the results for the individual misconceptions one after the other in distinct subsections. Last but not least, we discuss limitations of this user study.

4.3.1 Overall findings. The prevalence of the different misconceptions varies greatly. Despite being reported in the literature review, several misconceptions did not seem to be prevalent in our sample, as evidenced by the ceiling effects found for M5, M13, M15, and M16. Still, our interventions led to a significant decrease in the overall prevalence of the identified misconceptions, since most of the other misconceptions could be addressed by our developed interventions.

Most of the misconceptions not affected by the ceiling effects could be addressed by the intervention we created leading to significant increases in the portions of correct responses between the pre-treatment questionnaires and the post-treatment questionnaires (10 out of 16). However, the results with respect to several misconceptions warrant a closer inspection. On the one hand, the intervention texts for the six misconceptions M7, M12, M14, M17, M21, and M22 did not result in a significant improvement with respect to the prevalence of the respective misconception. On the other hand, despite exhibiting more than 90% of correct responses in the post-treatment questionnaire, the two misconceptions M9 and M19 misled more participants to an incorrect answer after the treatment, than they resulted in additional correct answers. Also, the elevated number of incorrect responses after the intervention with respect to misconception M2 warrant closer inspection. In the following, we discuss each of the aforementioned ten misconceptions individually in ascending order (i.e. M2, M7, M12, ...).

4.3.2 M2: The inclusion of symbols makes passwords automatically more secure. While M2 exhibits a significant improvement from the pre-treatment questionnaire to the post-treatment questionnaire, it reaches only 51.1% of correct responses. This is the lowest value among all misconceptions. Consequently, we argue that further refinements are required. We propose to add more concrete examples to the intervention texts, based on the studies reporting this misconception and common mangling rules used with password cracking software[1]:

Using specialized software, attackers try to mimick human behaviour when guessing passwords. They use a long list of words (from dictionaries, but also passwords from past breaches) and apply different common modifications to these words to generate additional words they will also use as guesses for the password. Such modifications are:

- *Appending or prepending numbers and symbols (e.g. adding an "!" to the end is a popular choice). Examples of passwords that can be guessed very quickly using such rules are "brooklyn16", "bubblegum1!", "1proudmom" or "Mamamia!!!".*
- *Substituting letters with numbers (e.g. E → 3) or with symbols (e.g. a → @). Examples of passwords that can be guessed very quickly using such rules are "p@ssw0rd", "L0vemetal", "m0nkeyl10n", or "4n4belle".*
- *Substituting lowercase letters with uppercase letters (in particular at the beginning of words). Examples of passwords that can be guessed very quickly using such rules are "pAsswOrd", "Thisismypass", "NOTSOSURE", "daywalker", or "Lovemetal".*

Therefore, using numbers, symbols, or uppercase letters in your password will not automatically make it harder to guess.

[1]Based on the winning contribution to the Best64 Challenge, aiming to find the most effective rules: https://hashcat.net/forum/thread-1002.html

4.3.3 M7: Reusing passwords is OK for passwords that are entered more frequently. M7 is part of one instance, where multiple interventions were combined into one during the iterative design (see Section 3). While a McNemar test did not show a significant improvement for M7, it did for the misconception addressed in the same intervention text (M6). Consequently, one might assume that the formulations addressing M6 might dominate M7. When inspecting the intervention text closely, it must be acknowledged that it is somewhat unbalanced, giving more room to M6 than to M7. Therefore, we propose the following more balanced formulation of the intervention:

Unfortunately, it happens time and again that even large web services handle the passwords of their users carelessly which then leak to attackers. Therefore, even passwords which are very hard to guess should not be reused. If a password is leaked by a service in the clear, it does not matter how hard it is hard to guess. How frequent you enter the password for a specific account does also not affect the security requirements of that account and warrant reuse of that password. Reusing passwords should always be avoided. The more often you reuse a password at different services, the bigger the chance of it getting into the hands of an attacker.

The other instances where the interventions of multiple misconceptions were combined into one did not seem to be affected by the same issue. In one instance (M1, M2, M3, M4) all misconceptions show a significant improvement after the treatment, in the other instance (M15, M16) no significant differences could be found (due to ceiling effects). Thus, the issue does not seem to be a general issue stemming from combining multiple interventions into one.

4.3.4 M9: Notes of passwords do not need to be particularly protected. M9 misled seven participants (i.e. seven participants having answered correctly in the pre-treatment questionnaire answered incorrectly in the post-treatment questionnaire). However, all five participants who answered incorrectly in the pre-treatment questionnaire, changed their answer to the correct one in the post-treatment questionnaire and the portion of correct post-treatment responses was 92.1%. Furthermore, the decrease in correct answers between the pre-treatment questionnaire and the post-treatment questionnaire was not found to be a significant difference. Thus, we argue that more testing of the intervention is required, before any further changes can be proposed.

4.3.5 M12: Keyboard patterns are secure passwords. Our analysis did not show a significant increase in correct answers for M12. Additionally, it exhibits the largest number of misled participants of all misconceptions (i.e. 10 participants), although the number of participants having answered incorrectly in the pre-treatment questionnaire and correctly in the post-treatment questionnaire is still larger (i.e. 16 participants). We believe this to be a surprising finding. The intervention text includes an explanation of the misconception and how an attacker can use it against the participants. To increase the clarity of this misconceptions formulation, we propose the following rephrased version:

Using walks or patterns on your keyboard as password (e.g. "1q2w3e4r" or "mnbvcx") is no good practice to generate secure passwords. As a matter of fact, such patterns will be among the first guesses of every attacker trying to guess passwords. Therefore, you should never use keyboard patterns as passwords, even if they conform to the password policy of a website or system and contain uppercase letters, numbers, and symbols.

4.3.6 M14: Attackers do not automate their attacks on passwords, but perform them by hand. Our analysis did not show a significant increase in correct answers for M14 as well. Due to the fact that this misconception applies to many possible attacks on passwords and user accounts, the intervention was formulated in an abstract manner with just two concrete examples. In order to make the underlying problems more tangible for lay users, we propose the following refinement with an additional example and a more concrete wording:

Attackers can easily automate their attacks and do not have to perform attacks manually by hand. Specialized software to e.g. test billions of different passwords in just one second after a successful break-in, build phishing websites that look just like the original, or snoop on passwords in unencrypted network traffic are readily available.

4.3.7 M17: Email is security-wise not an important service and therefore does not require a secure password. While helping 15 additional participants to understand M17, the respective intervention text did not result in a significant improvement in the post-treatment questionnaire. The text only covered one possible consequence, i.e. that attackers gain access to additional accounts by resetting the respective passwords, when they can be reset through emails (either by sending a reset link or by sending a new password). Thus, we propose the following refinement by including an additional consequence, i.e. sending malicious mails to acquaintances:

Even if you use your email account only to send messages to others, it is still a valuable target for attackers. On the one hand, exploiting the possibility to reset passwords of other accounts is particularly relevant. Your email account holds email from all the services you use. Therefore, attackers can easily look up all the web services you use and reset their passwords to access them. On the other hand, attackers can use your email account and the emails within it to determine your acquaintances and send emails with phishing links or attached malware to them in your name.

4.3.8 M19: It is not necessary to set a password to lock the screen of unattended devices. The results with respect to M19 were very surprising: before the treatment all responses were correct, but after the treatment some participants changed to incorrect responses. This indicates that there might be an issue with the intervention. However, since the decrease in correct responses was not found to be a significant difference and the portion of correct post-treatment responses was 94.4%, we argue that further investigations are required before further refinements to the intervention text can be proposed.

4.3.9 M21: The frequency of use of an account influences its security requirements. With respect to M21, no participants changed from their correct response in the pre-treatment questionnaire to an incorrect response in the post-treatment questionnaire. Yet, despite only two participants responding incorrectly after the treatment, our analysis shows no significant difference after reading the interventions. In addition, there is also no ceiling effect. The important aspect with this misconception is that users understand what exactly influences the security requirements of an account and what

does not. Therefore, we propose to substantiate the explanation with examples:

The value of your accounts is not influenced by how regularly you use it. Instead, the only determining factors are the data which can be accessed in the account (e.g. personal photos) and which actions can be performed in the account (e.g. sending messages to friends who trust you would never send them a malicious link).

4.3.10 M22: Bank accounts do not need to be protected with strong passwords if there is no money in them. Last but not least, M22 did not show a significant improvement in correct responses between the pre-treatment questionnaire and the post-treatment questionnaire. Yet, despite only one incorrect response remaining in the post-treatment questionnaire, there also was no ceiling effect. The underlying problem of this misconception is that attackers can perform different actions than withdrawing money from the account. Thus, we argue that additional examples might improve the intervention:

Money is not the only valuable associated with your bank account. When accessing your online banking account, attackers can easily see where you are shopping, when you book your holidays and where you are paying abroad, your address, your phone number… All they need is your password, no TANs are needed. Depending on your bank they might also change your overdraft limit, open additional accounts, or order additional banking cards.

4.3.11 Limitations. One limitation of our user study lies in the participant sample. All participants are lay users employed in German SMEs. Thus, it is unclear whether our findings fully translate to different groups of users. As future work, we plan to repeat the study in various contexts in order to verify the results there.

Also, due to the fact that the study was conducted following the recommendation of Haeussinger and Kranz [27] in the real work environment of the participating employees in three SMEs, the study setting could not be controlled. The participants were unsupervised throughout all three stages of the study, i.e. filling the pre-treatment questionnaire, reading through the interventions, and filling the post-treatment questionnaire. Thus, a number of limitations arise: (a) participants might have used the interventions while filling out the questionnaire, (b) participants might have filled out the post-treatment questionnaire after reading the interventions only partially, and (c) participants who work in the same SME might have worked (partially) together.

Additionally, the participants filled the post-treatment questionnaire directly after having read the interventions. Therefore, we have no data on the effectiveness after longer periods of time have passed. Further retention studies would be required to verify our results in this respect.

Last but not least, while the interventions significantly improved the prevalence of misconceptions in our study and the study was conducted in the employees' real work environment, it might be that the participation in the study has motivated the employees more than they would have been otherwise. In particular, the effectiveness outside the study setting and whether the decreased prevalence of misconceptions leads to more secure behaviour might depend on how the interventions are presented to the users and what information is provided alongside them.

5 CONCLUSION

In this paper, we lay the foundation to fight back against a decade of misconceptions about password security. We provide a list of the misconceptions about password security reported in the literature of the past decade. Thereby, we contribute to an increased awareness of these misconceptions among information security experts. Additionally, we provide formally evaluated interventions which address the identified misconceptions. The results of our user study show that the interventions can decrease the prevalence of many of the identified misconceptions significantly. However, we also find that some misconceptions are barely present in our sample as evidenced by the ceiling effects found in our analysis.

Future work includes the validation of our findings with larger participant samples. Thereby, it might be also of interest to compare the findings gathered in the organizational context with participants from the private context. Additionally, investigating the misconceptions reported in the literature before 2007 might provide insights how the mental models of text passwords have evolved over time and might prove to be an interesting line of future work.

6 ACKNOWLEDGEMENT

This work has been developed within the project 'KMU AWARE' which is funded by the German Federal Ministry for Economic Affairs and Energy under grant no. BMWi-VIA5-090168623-01-1/2015. The authors assume responsibility for the content.

7 LITERATURE RESEARCH REFERENCES

[1] Mohammed Awad, Zakaria Al-Qudah, Sahar Idwan, and Abdul Halim Jallad. 2016. Password security: Password behavior analysis at a small university. In *International Conference on Electronic Devices, Systems and Applications*. IEEE.

[2] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017).

[3] Shirley Gaw and Edward W Felten. 2006. Password management strategies for online accounts. In *Symposium On Usable Privacy and Security*. ACM, New York, New York, USA, 44–55.

[4] Eiji Hayashi and Jason I. Hong. 2011. A diary study of password usage in daily life. In *Conference on Human Factors in Computing Systems*. ACM, 2627–2630.

[5] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *USENIX Security Symposium*. 327–346.

[6] Michaela Kauer, Sebastian Günther, Daniel Storck, and Melanie Volkamer. 2013. A Comparison of American and German Folk Models of Home Computer Security. In *Human Aspects of Information Security, Privacy, and Trust*. Springer, 100–109.

[7] Birgy Lorenz, Kaido Kikkas, and Aare Klooster. 2013. "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 276–283.

[8] Ijlal Loutfi and Audun Jøsang. 2015. Passwords are not always stronger on the other side of the fence. In *Workshop on Usable Security*.

[9] Nathan Malkin, Marian Harbach, Alexander De Luca, and Serge Egelman. 2017. THE ANATOMY OF SMARTPHONE UNLOCKING: Why and How Android Users Around the World Lock their Phones. *GetMobile: Mobile Computing and Communications* 20, 3 (2017), 42–46.

[10] Gilbert Notoatmodjo and Clark Thomborson. 2009. Passwords and perceptions. In *Australasian Information Security Conference*. Australian Computer Society, Inc., 71–78.

[11] Fayyaadh Parker, Jacques Ophoff, Jean-Paul Van Belle, and Ross Karia. 2015. Security awareness and adoption of security controls by smartphone users. In *eCrime Researchers Summit*.

[12] Caitlin Rinn, Kathryn Summers, Emily Rhodes, Joël Virothaisakun, and Dana Chisnell. 2015. *Password creation strategies across high- and low-literacy web users*. American Society for Information Science.

[13] M A Sasse, S Brostoff, and D Weirich. 2001. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security - Springer. *BT Technology Journal* 19, 3 (2001), 122–131.

[14] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Designing Password Policies for Strength and Usability. *ACM Transactions on Information and System Security (TISSEC)* 18, 4, 13–34.
[15] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords . In *USENIX Security Symposium*.
[16] Elizabeth Stobert and Robert Biddle. 2015. Expert Password Management. In *International Conference on Passwords*. Springer International Publishing, 3–20.
[17] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Conference on Human Factors in Computing Systems*. ACM, New York, New York, USA, 3748–3760.
[18] 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.
[19] Ding Wang, Debiao He, Haibo Cheng, and Ping Wang. 2016. fuzzyPSM: A New Password Strength Meter Using Fuzzy Probabilistic Context-Free Grammars. In *eCrime Researchers Summit*.
[20] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites. In *USENIX Security Symposium*.

ADDITIONAL REFERENCES

[21] Joseph Bonneau, Mike Just, and Greg Matthews. 2010. What's in a Name?. In *International Conference on Financial Cryptography and Data Security*. 98–113.
[22] J Bonneau and S Preibusch. 2010. The password thicket: technical and market failures in human authentication on the web. *WEIS '10: The 9th Workshop on the Economics of Information Security* (2010).
[23] Nathan Bos, Darren Gergle, Judith S Olson, and Gary M Olson. 2001. *Being there versus seeing there: trust via video*. ACM.
[24] Sonia Chiasson and P C van Oorschot. 2015. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography* 77, 2-3 (April 2015), 401–408.
[25] Dinei Florêncio, Cormac Herley, and Paul C van Oorschot. 2014. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *USENIX Security Symposium*.
[26] Paul A Grassi, Michael E Garcia, and James L Fenton. 2017. *Digital Identity Guidelines (Revision 3)*. Technical Report. National Institute of Standards and Technology.
[27] 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.
[28] Philip G Inglesant and M Angela Sasse. 2010. The true cost of unusable password policies. In *CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 383–392.
[29] National Cyber Security Centre. 2016. *Password Guidance: Simplifying Your Approach*. Technical Report.
[30] 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.
[31] PCI Security Standards Council LLC. 2016. Payment Card Industry (PCI) Data Security Standard (Version 3.2). (April 2016).
[32] Elena Rocco. 1998. *Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact*. ACM Press/Addison-Wesley Publishing Co.
[33] Bruce Schneier. 2005. Write Down Your Password. (May 2005). https://www.schneier.com/blog/archives/2005/06/write_down_your.html
[34] Elizabeth Stobert. 2014. The agony of passwords: can we learn from user coping strategies?. In *CHI EA '14*. 975–980.
[35] 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.
[36] Blase Ur, Sean M Segreti, L Bauer, N Christin, L F Cranor, Saranga Komanduri, Darya Kurilova, Michelle L Mazurek, William Melicher, and Richard Shay. 2015. Measuring real-world accuracies and biases in modeling password guessability. In *USENIX Security Symposium*.
[37] Rafael Veras, Julie Thorpe, and Christopher Collins. 2012. *Visualizing semantics in passwords: the role of dates*. ACM.
[38] Yinqian Zhang, Fabian Monrose, and Michael K Reiter. 2010. The security of modern password expiration: an algorithmic framework and empirical analysis. In *ACM conference on computer and communications security*. 176–186.

APPENDIX

Table 2: The items for each of the misconceptions, translated from the German originals used in the study.

ID	Item of the Intervention
M1	Adding numbers makes passwords automatically more difficult to guess.
M2	Adding symbols makes passwords automatically more difficult to guess.
M3	Adding uppercase letters makes passwords automatically more difficult to guess.
M4	Replacing lowercase letters in the password with numbers, symbols, or uppercase letters makes the password more difficult to guess.
M5	A word from another language than the your own mother tongue is a secure password.
M6	Reusing passwords is OK for secure passwords, but should be avoided for weak passwords.
M7	It is OK to reuse passwords from user accounts that you log in frequently for different user accounts.
M8	Security-wise, it is better to write passwords down and keep them in a secure location than to reuse passwords for different user accounts.
M9	Notes of passwords must always be stored in a secure location.
M10	Passwords should be changed frequently.
M11	Storing passwords in the browser is the same as storing passwords in a password manager.
M12	Walks or patterns on the keyboard (e.g., 1qay2wsx) represent insecure passwords.
M13	Using dates of birth that are not your own is a good way to choose secure passwords.
M14	Attacks on user accounts can be automated.
M15	All attackers are strangers from the other end of the world.
M16	All attackers are only people you know.
M17	Email accounts have particularly high security requirements.
M18	A SIM PIN is sufficient to protect data on a smartphone.
M19	It is necessary to lock your devices (PC, laptop, smartphone, etc.), even if you leave them unattended only for a short time.
M20	User accounts in an organization have lower security requirements than private user accounts, because the IT department watches over them.
M21	The security requirements of a user account depend on how often it is used.
M22	Only bank accounts with high account balance are a rewarding target for attackers.
M23	One can be too unimportant to be attacked.