User Behaviors and Attitudes Under Password Expiration Policies

Hana Habib, Pardis Emami-Naeini, Summer Devlin†, Maggie Oates, Chelse Swoopes,
Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University University of California, Berkeley (†)
{htq, pemamina, moates, cswoopes, lbauer, nicolasc, lorrie}@andrew.cmu.edu
devlins@berkeley.edu†

ABSTRACT

Policies that require employees to update their passwords regularly have become common at universities and government organizations. However, prior work has suggested that forced password expiration might have limited security benefits, or could even cause harm. For example, users might react to forced password expiration by picking easy-to-guess passwords or reusing passwords from other accounts. We conducted two surveys on Mechanical Turk through which we examined people's self-reported behaviors in using and updating workplace passwords, and their attitudes toward four previously studied password-management behaviors, including periodic password changes. Our findings suggest that forced password expiration might not have some of the negative effects that were feared nor positive ones that were hoped for. In particular, our results indicate that participants forced to change passwords did not resort to behaviors that would significantly decrease password security; on the other hand, their self-reported strategies for creating replacement passwords suggest that those passwords were no stronger than the ones they replaced. We also found that repeating security advice causes users to internalize it, even if evidence supporting the advice is scant. Our participants overwhelmingly reported that periodically changing passwords was important for account security, though not as important as other factors that have been more convincingly shown to influence password strength.

1. INTRODUCTION

Passwords are widely used for authentication, from individual online accounts to organizational access control. It is well known that people create passwords that are easily guessed [22, 37], and engage in insecure practices, such as reusing passwords across different accounts [7, 9, 32, 37]. Prior research has focused on helping users make stronger passwords through password-composition policies (e.g., [20]), which require users to include a defined number of characters and character classes in their passwords, and understanding the impact of password blacklists (e.g., [38]), which prevent users from creating passwords that are too common. The purpose of these password security tools is to help users create passwords that are less vulnerable to automated password guessing.

Historically, password expiration policies have been implemented to help prevent password guessing attacks [31]. At the time these policies were first proposed, computational power was far scarcer than it is now and a successful password cracking attack would have taken several months. Thus, changing passwords every month may have seemed to be a reasonable method for defeating such an attack [31]. Furthermore, password expiration could act as a failsafe mechanism to eventually lock out attackers who may have gained access to a legitimate user's password without their knowledge. As a result of those desirable properties, expiration policies, of varying duration, have become widespread practice, especially for university and government systems [10].

Research has demonstrated that given modern computing capabilities, expiration policies may have limited utility for organizational security, largely due to the predictability of human behavior in password management [3, 39]. Though it is known that people struggle to handle the demands of password management, we question the intuition that expiration policies lead users to choose simpler passwords than their existing ones or reuse passwords from other accounts at a greater rate. Our study complements a survey conducted by the U.S. National Institute of Standards and Technology (NIST) exploring the steps users actually take when they are forced to change their password [4]. We build on this prior work, which analyzed password behaviors of participants from a single U.S. government organization, by surveying participants from numerous and diverse workplaces from across the U.S., who face a variety of different organizational password policies and requirements. Additionally, we analyze how reported coping strategies differ for those who face more frequent expiration. We also contribute additional user perspectives related to expiration, such as how people prioritize password changes among other password-management practices.

Our results are largely consistent with those found in NIST's study [4], and suggest that despite users generally employing harmful password practices, frequent password changes do not lead to some of the negative security effects thought to be introduced by expiration policies. Based on their self-reported behaviors, we found that participants did not create passwords that are simpler than the ones they already

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

use or reuse passwords from other accounts at a higher rate. Though expiration policies do not appear to increase the incidence of account lockouts or lead users to change their password-recall strategies, participants reported relying on coping mechanisms, such as appending digits to their previous password, to update their password. Such coping mechanisms greatly reduce the potential security gains brought by expiration policies.

In general, our participants reported that password expiration had a positive impact on security, with 82% agreeing that it made it less likely that an unauthorized person will log in to their account. However, changing passwords periodically was thought to be less important for account security than creating a complex password, storing the password safely, and avoiding password reuse. This is in line with modern security guidance, such as the recent changes to the NIST authentication guidelines [12], which recommend against password expiration policies. With the additional insights gained in this study, it is evident that users accept and adapt to the security advice they are provided, especially if they hear it repeatedly from a trusted source, such as their employer's IT department. This suggests that, if communicated appropriately, users may be open to more updated recommendations, such as using password managers or enabling two-factor authentication.

In the remainder of this paper we first discuss literature relevant to our study. We then describe the study design and methodology used in analyzing the collected data. Next, we present our findings regarding password usage at work, update behavior, impact of different expiration policies, and security perceptions related to password expiration. Finally, we conclude with a discussion of our results.

2. RELATED WORK

There is a large body of literature pertaining to various aspects of password authentication. We discuss the prior work that is most relevant to our study, such as those examining password management, challenges due to password expiration, or security perceptions related to passwords. Our work builds upon this existing literature by analyzing what strategies people use to cope with password management, including password updates, and how they generally feel toward periodic password changes.

2.1 Password-Management Strategies

Users face considerable burdens in managing passwords. Previous research has found that people use over 20 passwords in their daily lives [9, 27]. A diary study conducted by Grawemeyer and Johnson observed that, on average, their participants logged into various accounts over 45 times in one week [13]. Authentications for work activities accounted for 43% of all logins in their sample, highlighting the importance of studying workplace password management behaviors in particular.

Prior work has also shown that people have varying strategies for selecting passwords [32, 34]. One common strategy for coping with multiple passwords is to reuse passwords across different accounts [7,9,32,34,37]. In a 154-participant empirical study of password usage, Pearman et al. observed that participants exactly reused passwords for 67% of their accounts and had passwords containing a string of at least four characters in common for 79% of their accounts [27]. The more passwords a user has created, the more likely they are to reuse passwords [11]. Previous research has also found that users attempt to match password strength to the relative importance of the account when selecting passwords [25, 34]. Stobert and Biddle further observed in an interview study that their participants rarely changed passwords on their own, and only did so in the case of a breach or forgotten password [32]. This literature motivates our research, which aims to understand how people cope with forced password changes in addition to the normal demands of password management.

Users also differ in how they recall their passwords, typically relying on their memory [11, 13, 32]. However, writing down at least some account passwords is also common practice [32]. Previous research has found the adoption of password managers to be low [16], even though they are widely recommended for password security [29]. Building upon this literature, our work tries to identify whether password recall, a major usability factor related to password use, is impacted by password expiration.

2.2 Password Expiration Challenges

In an empirical study of the password policies of 75 different websites, Florêncio and Herley found that 20% of the websites they examined required participants to update their password regularly [10]. Prior literature has shown that required password changes have negative implications for usability. Shay et al. found that only 30% of their survey participants created an entirely new password when forced to change their university password and 19% had issues recalling their new password [30]. Other user issues related to required password changes include being reminded to change a password too early, difficulty keeping track of updated passwords, struggling to create passwords that meet the institution's password requirements, and fear of being locked out of an account [8, 14].

A major security issue related to password expiration is the tendency for people to make predictable changes when updating their password, which can be exploited to optimize password-cracking attacks [1]. Zhang et al. developed a transform-based password-cracking algorithm, using password history data for 7,700 accounts at their institution. With the knowledge of the accounts' previous passwords, they were successful in guessing 41% of passwords in an offline attack and 17% in an online attack (allowing for a maximum of five guesses). Thus, they demonstrated that password expiration seems to have limited utility for locking out attackers who have already gained knowledge of a user's password [39]. Chiasson and van Oorschot further demonstrated that with modern computing capabilities and taking into account human behavior in password creation, it is no longer feasible to change passwords faster than they can be potentially cracked [3].

Most related to our study, a survey conducted by NIST explored password-management behaviors of 4,573 Department of Commerce (DOC) employees who had, on average, nine work-related passwords [4]. The authors estimated that DOC employees spent 12.4 hours per year changing passwords on a 90-day expiration schedule, or 18.6 hours changing passwords on a 60-day expiration schedule. The study also revealed that most employees coped with the burden of

password changes by making minor changes to their existing password. The authors found that positive attitudes toward password requirements (i.e., composition and expiration requirements) correlated with more secure behaviors and fewer usability problems. We build on this prior work by studying a population that includes users from a wider variety of workplaces with differing password policies. We additionally explore perceptions about expiration independently of other password requirements. Furthermore, we analyze usability patterns more deeply, such as the correlation between creation and update strategies, and whether certain techniques are associated with more frequent account lockouts.

More recent security recommendations have been moving away from password expiration policies [5, 6, 24, 40]. The NIST Special Publication 800-63B, Digital Identity Guidelines, was recently revised and now recommends that "Verifiers should not require memorized secrets to be changed arbitrarily (e.g., periodically)" and that they should only be changed in special circumstances, such as when there is a compromise of passwords [12]. However, the NIST standards are only required for U.S. government systems. Other prominent security standards, including the Payment Card Industry (PCI) Data Security Standards and ISO/IEC 27002, still recommend regular password changes [15,26]. Our work provides insight into the security mindset of workplace password users that can be used to inform future institutional password security recommendations.

2.3 Perceptions of Password Security

Previous research has also studied perceptions related to the security of passwords. In two separate studies, Ur et al. collected users' perceptions of password strength. They discovered that participants had some misunderstandings about what makes a password secure, including thinking that adding digits made their passwords stronger than it really did and that keyboard patterns and common phrases were more random than they actually are [33,34]. This often meant that users created passwords that did not match their desired security level, for example, creating weak passwords for highly valued accounts [33]. We expand on this work by evaluating user perceptions related to several password practices, instead of only password composition.

Furthermore, researchers have discovered that there is a disconnect between what people believe is beneficial to password security and what they actually do. Riley found a number of behaviors, such as changing passwords for accounts or using special characters, that the majority of their participants believed they should engage in, but did not do so [28]. Our study looks into perceptions about similar behaviors, but aims to understand the perceived relative importance of these behaviors.

In a survey comparing the security practices of experts and non-experts, Ion et al. reported that non-experts recommended using anti-virus software, creating strong passwords, visiting only known websites, and changing passwords frequently to stay secure online. Non-experts and experts both perceived using strong and unique passwords as effective security mechanisms and reported that they would be likely to follow those practices. Not writing down passwords was considered somewhat effective, while saving passwords in a file, using a password manager, and writing down passwords were considered ineffective security advice [16]. Through our work, we attempt to gain a deeper understanding of these perceptions in the context of workplace passwords.

Prior work has found that people also have misconceptions about protecting against different threats [32], often overestimating the threat of a targeted attack and underestimating that of automated guessing attacks [33]. For example, Gaw and Felten found that participants viewed password complexity and randomness as means to reduce human gussability and not necessarily as protection against an automated attack. Participants also viewed friends (and others close to them) as the most capable attackers, while hackers were perceived as the most motivated [11]. We evaluate the threats people consider in managing workplace passwords, and the role expiration policies play in these perceptions.

3. METHODOLOGY

In this study, we analyzed data collected from two separate online surveys. The first survey focused on people's workplace password habits, while the second measured perceptions of several password practices, including periodic password changes. We used both quantitative and qualitative methods to analyze data collected from the surveys.

3.1 Data Collection

In this section we describe the procedures for collecting our survey data. Both surveys were approved by our Institutional Review Board (IRB) and were conducted on Amazon's Mechanical Turk[1]. Participants were age 18 or older, residents of the United States, and had a HIT approval rate of over 90%.

3.1.1 Workplace Passwords Survey

The first survey in our study, which will be referred to as the ***workplace passwords survey***, was implemented as a screening survey followed by a full survey about participants' experiences with their workplace passwords. We implemented a screening survey to ensure that only participants who had at least one workplace password were allowed to answer questions in the full survey, as questions about a main workplace password would be irrelevant to those with no workplace passwords.

In the screening survey, participants answered a total of six questions that asked how many workplace passwords they have and their age, gender, ethnicity, education, and occupation. Those who met the qualification criteria of having at least one workplace password were contacted through Mechanical Turk about completing a "bonus survey," which was the full survey about workplace password habits. Questions included in the screening survey are in Appendix A.

The full survey was designed to ask participants about their experiences with their main workplace account and included 31 multiple-choice and five open-ended-response questions. With these questions we explored workplace password habits, such as experiences creating, updating, and recalling passwords, as well as sentiments toward password expiration. In this survey, we confirmed the four demographic attributes participants provided to us in the screening survey. We also included an attention-check question that was a duplicate of

[1]Amazon's Mechanical Turk. `https://www.mturk.com`

the question asking participants how many workplace passwords they have. The full survey is provided in Appendix B.

A total of 618 people submitted the screening survey and 407 finished the full survey. Participants were compensated $0.25 for the screening survey and $2.00 for the full survey. On average, participants finished the screening survey in about two minutes and the full survey in 10 minutes.

3.1.2 Password Perceptions Survey

The second survey we conducted, which will be referred to as the ***password perceptions survey***, explored people's perceptions of the relative importance of four password practices: *using a complex password*, *storing the password in a safe place*, *creating a password that you do not already use somewhere else*, and *periodically changing passwords*. In the survey, participants rated the importance of each of these practices for account security on a five-point Likert scale, and completed open-ended responses explaining their ratings. We also asked participants to rank failure to adhere to each practice (e.g., using a simple password) in order of harm to account security. Participants were then shown pairs of the practices and then were asked to indicate whether one contributes more to account security than the other. Lastly, we asked participants about their anticipated behaviors in a hypothetical scenario in which their workplace implemented or removed an expiration policy (depending on the participant's current workplace policy). The order of the four password practices was randomized in each section to avoid biasing participants based on how the practices were presented. Appendix C contains the questions in this survey.

People who completed the workplace passwords survey were disqualified from taking this survey. The password perceptions survey was completed by 340 eligible participants who were compensated $1.50. On average, participants completed the survey in about 10 minutes.

3.2 Data Analyses

This section describes the statistical tests and qualitative methods used in analyzing the collected data. Data from the two surveys were analyzed separately.

3.2.1 Quantitative Analyses

Prior to running statistical tests, we excluded participants with inconsistent or obviously fraudulent responses to improve the validity of our analyses. For the analyses of data from workplace passwords survey we excluded 49 participants who answered the attention-check question inconsistently, one participant who reported that they did not change their main workplace password (even though they reported that they were required to change all of their workplace passwords), and one participant who selected every answer option for all questions where participants could select multiple options. It is possible that the attention-check question may have led to the exclusion of participants who simply misremembered their workplace passwords, and not just those who truly were not paying attention to the survey. We excluded only one participant from the analyses of data from the passwords perceptions survey as they used the same unintelligible response for each of the open-ended questions. Thus, 356 responses from the workplace passwords survey and 339 from the password perceptions survey were included in our analyses.

We conducted several different statistical tests and used significance level $\alpha = .05$ in our analyses. For categorical data, we used Pearson's chi-squared tests to determine the independence of two nominal variables, or Fisher's exact tests if counts in the contingency table were below five. For tests in which we were examining the impact of expiration frequency, we binned policies into three expiration periods: less than or equal to every 30 days, every 60 days, or greater than or equal to every 90 days. We report the phi coefficient (ϕ) to understand the effect size of the associations found for two binary variables, or Cramer's V (V) if the variables have more than two levels. Both measures are reported on a scale from -1 to 1, such that 1 demonstrates a complete positive association and -1 demonstrates a complete negative association between two variables. We report only statistical results for which we observed at least a small effect (demonstrated by an association of at least .1), which is a recognized threshold for statistical reporting [23].

To analyze data with a categorical independent variable and ordinal dependent variable, such as Likert-scale data, we used Kruskal-Wallis tests. We conducted a Friedman test to test the null hypothesis that password practices were rated as equally important. We also ran one-sample, two-sided Wilcox Signed-Ranked tests to determine whether participants felt one practice contributes more to account security than another by coding the rating options from -3 (left contributes much more) to 3 (right contributes much more), and testing the null hypothesis that the practices have equal contribution (a rating of 0).

In order to evaluate the impact of demographics on the use of password-creation, update, and recall techniques, we ran binomial logistic regressions where the independent variables were age, race, education level, and technical expertise, and the dependent variable was whether or not a certain technique was used. We ran binomial logistic regressions to determine whether password-creation techniques were predictors of update techniques, where the independent variables were one of 17 password-creation techniques (represented as binary variables) and the dependent variable was a password-update technique. For each significant factor found in the regressions, we followed up with chi-squared tests to determine the strength of the association between the factor and the dependent variable.

To analyze whether our participants used certain techniques for password memorability and others to make their password stronger, we ran a multinomial logistic regression. The dependent variable was a nominal variable with four levels: whether the update technique was used for making a stronger password, making the password easier to remember, both security and memorability, or neither security nor memorability. The baseline for the regression was set to neither security nor memorability. The independent variables were the password-update strategies measured in the survey.

3.2.2 Qualitative Analyses

Our surveys collected several open-ended responses which were each systematically analyzed to extract major themes. For each question, one researcher first developed a codebook based on common themes occurring in a sample of 20 responses. Two researchers then coded a random sample of 20% of the responses based on the first iteration of the

codebook. The researchers then reviewed their conflicts and revised the codebook accordingly. If agreement between the two coders, measured by Cohen's kappa, was less than $\kappa = .70$, a recognized acceptable threshold for agreement [36], both researchers recoded the sample and revised the codebook until reaching sufficient agreement. After successfully converging on the samples, one researcher would code the remaining responses for that question. Both researchers coded the full set of data collected for opinions on the impact of password expiration policies and reasons for continuing password changes. For the remaining qualitative data, the two researchers reached $\kappa = .81$ agreement, averaged over all questions. The statistics from qualitative responses reported in this paper are derived from the researchers' coding of the full set of responses.

3.3 Limitations

One of the major limitations of our study is that we recruited participants from Mechanical Turk. Though our participants come from a well-studied convenience sample, they may not reflect the behaviors and attitudes of the general population. Moreover, Mechanical Turk participants have been shown to be more privacy-sensitive than the population at large [17]. However, Mechanical Turk has proven to be a source of high-quality human subjects data [18], and has been successfully used in numerous studies related to passwords (e.g., [16, 20, 33]). Only 6% of our expiration survey population reported that Mechanical Turk was their primary occupation, indicating that the vast majority of participants were reporting on passwords for a different workplace.

Additionally, our study uses self-reported data about participants' past behavior, which participants may not have remembered or reported accurately. The effects of this may have been exaggerated by the privacy paradox, a well-studied observation that people's privacy attitudes often differ from their actual behaviors [19]. It is possible that our participants' reported reactions and attitudes toward password expiration may be different from their actual behaviors when facing their own expiration policies. While our data may be impacted by these limitations, we believe that our study is still a step forward in understanding people's general behaviors and attitudes related to password expiration.

4. RESULTS

Our surveys included questions about how people create, update, and manage their workplace passwords, as well as their attitudes toward password expiration in relation to other password-management practices. Similarly to participants in NIST's study [4], our participants generally reported coping with their expiration policy by modifying their current password, suggesting that updated passwords may not be any stronger or weaker than the ones originally created.

We also found that self-reported behaviors and attitudes related to expiration were largely independent from the presence and frequency of an expiration policy. Participants viewed password changes as important for account security, but felt that other password-management practices, such as using a complex password, storing the password safely, and avoiding password reuse were more vital. Our results indicate that while people may buy into security advice, they are sometimes unable or unwilling to act on the advice in a way that significantly improves password security.

4.1 Password Usage at Work

In this section we describe expiration policies reported by our participants and their password strategies for managing their main workplace password.

4.1.1 Password Expiration Policies

In total we analyzed data collected from 695 participants. The demographics of our participants are described in Table 1. On average, participants in both surveys reported having between three and four workplace passwords. 51% of participants in the workplace password survey reported that they were required to change most or all of their workplace passwords. Figure 1 shows the distribution of our participants' reported password expiration policies. The most common expiration period observed in our samples was expiry every 90 days, reported by 28% of participants in the workplace passwords survey and 19% of participants in the password perceptions survey. A larger percentage of participants in the password perception survey (59%) reported that they did not have an expiration policy for their main workplace password, compared to those in the workplace password survey (26%). It is possible that the wording of the recruitment text and questions in the workplace passwords survey primed participants to think more about expiration and report on their workplace passwords that did expire.

Almost two-thirds of participants (64%) from the password perceptions survey who did not have an expiration policy reported that they changed their workplace password periodically, while a large minority (34%) reported that they never changed it. Those who did change their password primarily mentioned account security in their explanations for doing so, while those who did not change their password most frequently mentioned that they never felt they had a reason to be concerned about the security of their account. In contrast, 53% of participants in a study conducted by Riley did not change their passwords on a regular basis. However, the survey was not specific to workplace passwords [28].

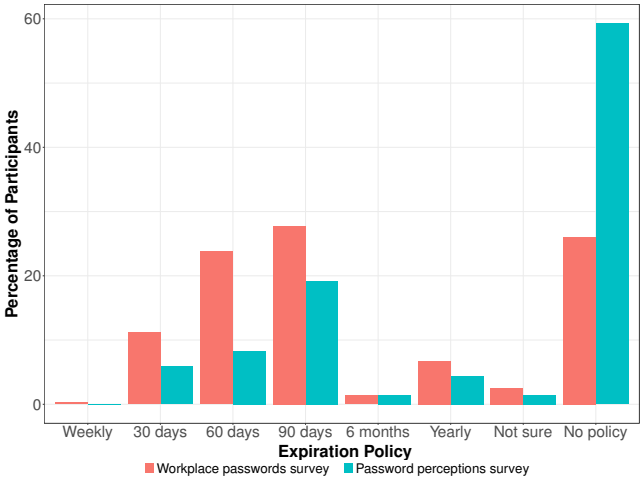

Figure 1: Percentage distribution of participants' workplace password policies. While a larger percentage of participants in the password perceptions survey did not have a workplace expiration policy, note that question wording and recruitment text differed between these two surveys.

Gender			Age			Education			Race		
	WP	*PP*		*WP*	*PP*		*WP*	*PP*		*WP*	*PP*
Female	51.7%	45.4%	18-24	6.2%	15.0%	Some high school	.3%	.6%	American/Alaska Native	1.4%	0.0%
Male	47.5%	53.1%	25-34	40.2%	46.3%	High school	7.9%	15.0%	Asian	5.6%	5.6%
Other	.3%	.6%	35-44	29.2%	23.9%	Some college	24.2%	28.3%	Black/African American	7.0%	7.4%
No answer	.6%	.9%	45-54	16.0%	8.3%	Associates	12.9%	13.9%	Hispanic/Latino	5.6%	8.0%
			55-64	7.6%	5.9%	Bachelors	36.0%	33.0%	Non Hispanic	.3%	.3%
			65-74	.6%	.3%	Graduate	17.7%	8.8%	White/Caucasian	77.0%	76.1%
			No answer	.3%	.3%	No answer	1.1%	.3%	Other	1.7%	1.5%
									No answer	1.4%	1.2%

Occupation						Tech Expertise		
	WP	*PP*		*WP*	*PP*		*WP*	*PP*
Business, Management, or Financial	24.2%	9.7%	Medical	6.2%	2.7%	Expert	9.3%	19.2%
Administrative Support	15.4%	10.9%	Mechanical Turk Worker	5.6%	12.7%	Non-Expert	88.5%	80.8%
Education/Science	12.6%	8.3%	Art, Writing, or Journalism	4.5%	7.7%	No answer	2.2%	0.0%
Service	11.5%	11.8%	Other	8.4%	19.8%			
Computer Engineering/IT Professional	9.3%	14.4%	No answer	2.2%	2.1%			

Table 1: Demographic breakdown of our participants from the workplace passwords (WP) survey, and the password perceptions (PP) survey.

4.1.2 Password Creation and Reuse

Our participants reported using common strategies to create their initial passwords, and on average indicated combining three password-creation techniques. The most common self-reported techniques used were using a word in English as part of their password (41% of participants), using a name (37%), and adding numbers (59%) or symbols (32%) to the beginning or end of a word or name. These were also common password-creation strategies observed by Ur et al. [34]. There were some demographic differences in the use of creation strategies. For example, participants ages 45 to 54 years old reported significantly less password reuse (both exact and with modifications) than participants who were 18 to 24 years old (exact: $p = .001, V = .24$, modified: $p = .001, V = .22$). Additionally, those who reported their race as Hispanic or Latino were slightly less likely than white or Caucasian participants to use an English word as their password ($p = .02, \phi = .13$). We also observed that technical participants (those who had ever held a job or received a degree in computer science or any related technology field) were slightly more likely to add symbols to the beginning or end of their password ($p = .05, \phi = .12$) and substitute symbols for letters ($p = .002, \phi = .18$). Participants also reported a moderate amount of password reuse for their main workplace password: 44% said their main workplace password is similar or identical to other work passwords, 57% reported that their main workplace password is very different from their non-workplace passwords.

4.1.3 Password Recall and Lockouts

Our participants had varying strategies for recalling their workplace password. The most common recall technique reported was memorizing the password, which was used by 53% of participants in the workplace passwords survey and 57% of participants in the password perception survey. Other work has also found password memorization to be users' dominant strategy for recalling a password [11, 13, 32]. In both of our surveys, over 85% of password memorizers reported having no backup method for recalling their passwords. Though participants in NIST's study also most frequently recalled their password through memory, over 80% also reported having stored their passwords on paper or electronically [4]. The most common password-storage technique reported by our participants was writing it down on paper, used by 19% of participants in the workplace passwords survey and 10% of participants in the passwords perceptions survey. However, one memorizer reported relying on a "change password" feature as a form of backup for their main workplace account, saying "I have good enough memory and use resetting as a backup." There were some demographic differences observed in the use of recall methods, but none were consistent across the two surveys.

The majority of participants (55%) reported memorizing their main workplace password within the first two times they logged in to their account. However, those who used a password manager ($p < .001, V = .41$) or wrote down their password ($p < .001, V = .22$) were significantly more likely to take more than two logins to memorize their password, on average learning their passwords after three to five logins. A quarter of participants who used a password manager reported that they did not memorize their passwords.

Overall, 45% of participants experienced at least one account lockout in the past year, with 12% reporting three or more lockouts. Participants in NIST's study appeared to face a similar lockout rate, as 48% viewed getting locked out as causing "some" or "a lot" of frustration [4]. Based of their reported lockouts, we found that participants who stored their password in their browser or wrote it down were two to three times more likely to face three or more account lockouts in the past year, while those who memorized their passwords generally faced fewer lockouts. Statistical results for the correlation between recall methods and account lockouts are reported in Table 2.

The most common password-recovery options reported by participants were calling someone on the phone (34%), sending someone an email (31%), and using a website (24%). Ten participants reported using their own method for recovering their main workplace password if they were unable to recall it, such as an encrypted USB drive or a piece of paper that they locked in a safe.

4.2 Password-Update Behavior

In this section we describe the self-reported strategies our participants indicated using during password changes, and

Recall Method	p
Web Browser	.001∗
Encrypted File	.55
Password Manager	.17
Password Protected Computer or Device	.30
Device or Computer Used Only by the Participant	.77
Write Password on Paper	.008∗
Write Reminder for Password	.72
Memorize Password	<.001∗

Table 2: P-values for chi-square tests comparing password-recall methods with the number of account lockouts. All tests had an effect size of $\phi = .24$. Significant results are marked with an asterisk

their reasons for using them. Participants primarily reported modifying their previous password during their last password change, and less than a quarter created one that was completely new.

4.2.1 Most Modify Their Previous Password

Table 3 displays the update strategies participants indicated using during the most recent change of their main workplace password. Participants typically indicated using one or two of these techniques to update their password. 237 (67%) participants reported creating their new password by modifying their previous one. The most common technique reported by our participants to modify the existing password was capitalizing a letter, which was used by 30% of participants. Only 37 (10%) participants reported that they reused passwords from other accounts during their last update, while 162 (46%) of participants reported updating their main workplace password with one that was completely new or using a password generator to create a new one. However, 76 of these participants also selected at least one modification technique with this option. Therefore, we estimate that only 24% of participants updated their password with one that was completely new. Similarly, 68% of participants in NIST's study generated a new password by making a minor change to their old one [4]. However, the NIST study appeared to have a larger degree of password reuse compared to our study population, as 43% of participants generated frequently used passwords by using existing ones.

Some participants described unique approaches for coping with their password expiration policy. For example, one participant reported that they used information from a fast food receipt as their password and used a new receipt to update their password. Demographics also had some impact on the use of update techniques. Most notably, we observed that age had an impact on reusing passwords from other accounts during password updates ($p = .03, V = .20$). On average, only 9% of participants ages 25 to 44 and 4% of those 55 to 64 reported that they reused password from other accounts in their last update, compared to 29% of participants who were 18 to 24 years old.

4.2.2 Creation & Update Strategies Are Consistent

Some initial password-creation strategies were significant predictors for the use of similar update techniques. For example, participants who reported that they used a password generator to *create* passwords were 18 times more likely than those who reported using other password-creation methods to use a generator to *update* their passwords ($p < .001, \phi = .48$). Additionally, those who reported substituting letters with symbols during password creation were seven times more likely than those who did not to report using the same technique to update their password ($p < .001, \phi = .35$). Those who reported using a birthday when creating their main workplace password were four times more likely to report using a date to update it ($p < .001, \phi = .26$). Password reuse was also consistent, as participants who reported exactly reusing a password from another account for their initial password were four times more likely to report reusing a password when updating ($p < .001, \phi = .28$) and those who reported reusing another password with modifications were three times more likely to report reusing a password at update ($p = .002, \phi = .19$). Our participants generally used the same strategy whenever they updated their passwords. In particular, 64% of participants reported using their strategy every time or most of the time when updating their password, while only 4% reported that they use very different techniques each time.

4.2.3 Techniques Associated with More Lockouts

The only update method that had an impact on password memorization was the use of a password generator. Those who reported using a password generator were twice as less likely to report that they memorize their password ($p = .007, \phi = .20$) and seven times more likely to report that they use a password manager to store their password ($p < .001, \phi = .20$), compared to those who did not use one. Two techniques correlated with a higher number of account lockouts. Those who reported that they duplicated characters during their last password update were three times more likely to report that they faced three or more account lockouts in the past year ($p = .005, \phi = .28$) and participants who reported substituting digits or special characters with the same character type were twice as likely to report having three or more lockouts ($p = .04, \phi = .28$), compared to those who did not use these techniques.

4.2.4 Motives & Reminders

Our participants had varying sources and motivations for using their update techniques. 47 of our participants shared where they learned their update strategy. Of these participants, 28% reported learning it from the Internet. Overall, 35% of participants used their strategy because it made their password easier to remember. Reusing a password was largely correlated with using the strategy for memorability ($\beta = 1.13, p = .007$). A quarter of participants reported that they used their strategy because they thought it made their password stronger. Based on the self-reported strategies, we observed that creating a new password ($\beta = 1.32, p < .001$) and using a password generator ($\beta = 2.00, p < .001$) during a password update were correlated with wanting to make the password stronger. Comparatively, memorability was more important to participants in NIST's study, as 81% cited using their password generating strategy so that their password was easy to remember.

We also asked participants about any reminders they receive when their password is about to expire The most common form of password change reminders reported were automated emails and software installed on their computers. We found that the timing of when the last reminder is sent did not have an impact on the effort participants reported

Technique	Example	Responses	%
Modifications			
Capitalizing a character	candy# → candY#	108	30.3%
Incrementing a character	dance#7 → dance#8	61	17.1%
Adding a sequence	dance#7 → dance#789	52	14.6%
Adding a date	raven → raven2016	44	12.4%
Substituting digits/special characters with the same character type	tar!heel1 → tar!heel4	42	11.8%
Moving a letter, digit or special character block	$steve27 → 27$steve	38	10.7%
Duplicating digits/special characters	password1! → password11!	34	9.6%
Substituting letters with matching characters	raven → r@ven	29	8.1%
Deleting digits/special characters	alex28!!! → alex28!!	23	6.5%
Substituting digits/special characters with the "shift" character for the same key	l00py*!2 → l00py*!@	17	4.8%
Changing a small part of the previous password in a way not mentioned		43	12.1%
Other Methods			
Creating a completely new password		139	39.0%
Reusing old passwords from other accounts		37	10.4%
Using a password generator		23	6.5%
Using a different approach		8	2.2%

Table 3: Techniques participants used to update their main workplace password during their most recent password change (which may or may not have been due to an expiration policy). On average, participants used one or two modification techniques for changing their password.

spending in updating their password. However, those who received password change reminders that were not software based were two times more likely to report spending additional effort in updating their password, compared to those who did receive software reminders.

4.3 Expiration Frequency Has Little Impact

We generally observed that the presence and duration of an expiration policy had only a relatively minor impact on password-management behavior. There were some differences in the impact to password recall in the data collected from the workplace passwords survey, but these differences were not observed in the passwords perception survey. For example, we found that 15% of participants with an expiration policy for their main workplace password reported storing their password in their web browser, compared to 5% of participants without a policy, which was found to be significantly different ($p = .02, \phi = .16$). However, the self-reported use of this storage method did not significantly differ between different frequencies. We also found that 40% of participants who stated that they faced a 60-day expiration policy reported memorizing their password, compared to 59% who reported longer expiration periods and 68% who reported facing shorter expiration periods, which was also a significant difference ($p = .003, V = .11$). Furthermore, we found that neither the presence nor duration of an expiration policy impacted the number of reported account lockouts.

We found that different expiration periods did not have an impact on the self-reported strategies participants used to update their main workplace password. Moreover, we found that the presence and frequency of an expiration policy did not impact whether participants reported making their main workplace password similar to passwords they use for other accounts (both workplace and non-workplace related). This suggests that people who face frequent expiration are not more likely to reuse passwords from other accounts.

The majority of our participants reported that they did not find updating their password difficult, but 60% agreed or strongly agreed that it was annoying. The reported frequency of their expiration policies did not impact participants' sentiments toward updating their workplace password. This finding suggests that users adapt to the requirements placed on them, but still find them burdensome.

4.4 Security Perceptions

Participants in both the workplace passwords survey and password perceptions survey considered password changes important to the security of their workplace account. However, periodic password changes were viewed as less important than using a complex password, storing the password safely, and avoiding reusing password. Our results suggest that people accept the security advice provided to them, especially if from a trusted source such as the IT organization of their employer.

4.4.1 Secure But Annoying

In their responses to the workplace passwords survey, 82% of participants agreed or strongly agreed that "frequent password expiration makes it less likely that an unauthorized person will break into my account." Neither the self-reported existence nor duration of an expiration policy significantly impacted participants' agreement with this statement. However, 66% of participants thought that their updated password was about the same strength as their old one, and only 25% thought it was stronger, suggesting that many may not be exerting extra effort into making their password stronger when they change it. This is consistent with the strategies participants typically reported to modify their passwords.

Participants' self-reported update strategies were generally independent from their opinion about the relative strength of their new password, with the exception of capitalizing a letter which was positively correlated with thinking the updated password was stronger ($p = .008, \phi = .12$). Since some update strategies (specifically using a new password and using a password generator) were reportedly used for making the password stronger, participants who reported using these techniques could also have used them in the past and thus felt that their password strength did not change.

4.4.2 Participants' Threat Models

When asked why expiration prevents unauthorized account access, in their open-ended responses a small majority (54%) stated that expiration prevented password compromise. Of those, around a fifth specifically indicated that expiration helps with security by reducing the time window for an attacker to figure out their password. One participant reported, "It takes time to hack or steal a password and if it is changed frequently it is less likely that the hacker will have time to obtain the password." Twenty-eight percent of participants also reported that expiration is beneficial *after* a password, whether new or old, has already been compromised. Around half of these participants reported more specifically that the main benefit of expiration policies is that they reduce the time an illegitimate user has access to the account after they have logged in. To this effect, one participant said that, "There will be less time for a hacker to retrieve your information." Interestingly, of those that disagree with expiration's benefits, most (66%) cited concerns that expiration is insecure or ineffective, while only a small group (10%) cited inconvenience or unproductivity in their text responses.

While discussing potential threats, most participants mentioned concerns about hackers, general unauthorized users (e.g., "people", "attacker,") or guessers; 5% explicitly mention current or former employees as a concern. Around 5% also expressed that expiration would minimize the impact of employees sharing their workplace passwords. It should be noted that participants appear to use the word "hacker" in a broad, colloquial sense beyond the concept of hackers as phishers or computational guessers. It was usually impossible to tease out their conception of "hacker" or "hacking." For example, one participant reported, "I had an exboyfriend hack my Facebook because my password was not strong enough." When asked the open-ended question why a workplace might implement an expiration policy, participants' reasons generally aligned with their responses to the question about the general impact of password expiration.

4.4.3 Desired Policies

Only 10 of the 260 participants who had an expiration policy in the workplace passwords survey expressed the opinion that their passwords should never expire. Otherwise, participants were most likely to recommend their own workplace expiration policy as the appropriate policy ($p < .001, V = .55$). Similarly, only 10% of participants in NIST's study recommended a less frequent change cycle, compared to their current 60- or 90-day policies [4]

In their qualitative responses to *why* the policy they chose was the best, most participants could not really articulate the reason. For example, 13% responded with a sentiment that the time period they selected was "just right." A third of participants said that the expiration period they recommended balanced security with either usability (mainly the ability to remember passwords) or convenience concerns. Most users seemed to be able to reconcile their concerns with the benefits of added security. One participant who recommended a policy of every 60 days explained, "Every 30 days is too frequent. I often forget my password because it's always changing. I do however understand that security is important, so passwords should be changed somewhat frequently." Participants who picked shorter time periods (e.g., 30 days) cited a security reason more often than participants who picked longer ones (e.g., a year), who more often cited a balance of security/usability or security/inconvenience. A small fraction of participants also cited employer or industry norms as part of their recommendation, with responses like "It's the standard we use and it works well."

4.4.4 Relative Importance of Password Changes

Participants in the password perceptions survey generally viewed creating a complex password as the most important practice for account security, followed by storing the password in a safe place and creating a password that is not already used for another account. Changing passwords periodically was reported to be the least important of these practices ($p < .001, V = .14$). Figure 2 shows the distribution of responses for how important each behavior was perceived. Demographics, including technical expertise, did not impact opinions significantly. Additionally, participants' views were found to be independent of whether or not they had a workplace expiration policy.

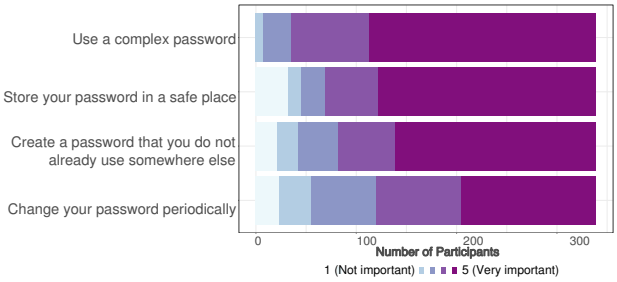

Figure 2: Distribution of ratings for each password-management practice studied. Participants viewed using a complex password the most important of these practices and changing passwords periodically the least important.

In qualitative responses explaining their rankings, participants mentioned usability concerns in roughly equal proportions for changing passwords, creating complex passwords, and avoiding password reuse. In line with their quantitative rankings, participants pointed out more downsides, such as it being inconvenient, insecure, unusable, or ineffective, for periodic password changes than other security practices. For example, one participant explained, "I don't think [periodic password change] is as important as people say...A really strong password doesn't just automatically become weaker simply because you've been using it for a while."

Also in line with the quantitative rankings, 5% of participants reported that a sufficiently complex password renders other practices less important, giving reasons like, "I don't believe it's necessarily important to change your password, if you have a secure one in the first place" or "If the password is good you should be able to [re]use it as much as you want as long as it is good." However, there were indications from the responses that users do not fully understand what comprises a good password, citing that "[...] a long nonsensical sentence works better and is more easily remembered, e.g., securitycomplexitymakesmypasswordssecurebutveryannoying." Lastly, some participants admitted that their attitudes and actions do not always align. Consistent with prior work, 2% volunteered that they believe they *should*

change their password or avoid reuse and that those practices are at least somewhat important, but that they do not do them [28]. When explaining their ranking for avoiding password reuse, one participant said, "It's important, but I do it [reuse passwords] anyway."

4.4.5 Hypothetical: Reversing Expiration Policy

In the hypothetical scenario in which the participant's workplace removed their expiration policy, almost half reported that they would continue changing their passwords periodically, be more likely to use a complex password, and be just as likely to avoid reusing passwords from other accounts. From the qualitative responses, reasons for continuing password changes were centered around it being a habit or beneficial for security. For example, one participant stated, "It's just a natural habit to do now for my own security." Those who stated they would not continue changes generally felt that it was too inconvenient or they would forget to do it if it was not required. As one participant put it, "I would forget as it is not on my high priority list."

From the quantitative data, half of participants who stated that they do not currently have a workplace expiration policy reported that they would be just as likely to use a complex password if their main workplace password expired periodically. Twenty-eight percent of participants who stated that they currently memorize their password reported they would no longer do so if periodic password changes were required. Almost half reported they were just as likely to create a password that is not used somewhere else. These results further highlight that password expiration may not contribute to a larger degree of password reuse, but likely does not encourage people to create more complex passwords during updates.

5. DISCUSSION

Our findings confirm that the strategies people use to adapt to their expiration policy are predictable. The majority of our participants reported coping with password changes by applying a simple modification to their current password. Our results are largely in line with NIST's study of the password-management behaviors of DOC employees [4]. However, our findings related to password reuse and backup recall methods do diverge, and may be attributed to the intense password burdens faced by DOC employees. Our results are also supported by Zhang et al. study, in which they were able to crack a substantial portion of their organization's passwords using the password history for the account [39]. This suggests that people in their organization were also typically using variations of their password during password updates.

Some participants reported using other coping strategies, such as cycling through a dedicated set of passwords for that account. Less than a quarter created a completely new password when it expired, a rate similar to that found by Shay et al. [30]. However, we did not find evidence that the self-reported strategies people use to update their password leads them to have weaker passwords. Furthermore, we observed that more frequent password changes did not lead to more self-reported reuse of passwords from other accounts. These results suggest that the negative security implications related to expiration may be limited to the case where there has already been a breach of an organization's passwords. In such cases, an attacker who knows a user's expired password may be able to easily guess the new password.

Our results also reveal that people generally do not have extremely negative reactions toward workplace password expiration, nor do they report significantly more usability burdens with more frequent password changes. Participants who reported facing more frequent expiration did not report experiencing a higher rate of account lockouts nor were they less likely to report memorizing their passwords than participants who reported facing less frequent password expiration. In addition, participants reported the same level of annoyance with updating their passwords, regardless of their self-reported password expiration frequency. This may be due to the fact that people adapt to expiration policies imposed by workplaces, often employing coping strategies that may reduce security in the event that their password is already known to an attacker.

In other scenarios, the presence of an expiration policy has little impact on security, even though a large percentage of participants held the view that updating their password would prevent hackers from cracking their passwords. Some participants even directly mentioned that they felt people will choose more creative passwords if they have to keep changing them. However, our results indicate that expiration largely does not influence people to create stronger passwords. Thus, password expiration likely provides no additional protection against an attacker with the modern computing resources to launch an automated guessing attack, even if the attacker does not have prior knowledge of the organization's passwords.

A few participants expressed concerns about targeted attacks in which a coworker or former employees of their organization would try to guess their password. Prior work has found targeted attacks to be a prevalent attack scenario that people worry about when managing their passwords [11,32,33]. Some were especially concerned about targeted attacks because they believed that sharing workplace passwords with coworkers was common practice. However, it is likely that expiration provides limited benefits even in the case of targeted attacks, since attackers may already know which modifications are typically used by their target.

Based on our results, we recommend that organizations consider whether the minimal security gains are worth implementing an expiration policy. Expiration policies may be attractive to organizations that have a history of password sharing among employees. Though expiring passwords may solve the immediate problem of system access to former employees, these organizations could be better off considering more secure mechanisms for enabling the collaboration between employees that causes password sharing. The benefits gained by avoiding attacks that are actually preventable by having an expiration policy must be weighed against a number of costs associated with implementing a policy, though our findings suggest that costs due to user burden are minimal considering current password-management demands.

Our second recommendation is that organizations implement enterprise password managers. In their existing implementations, expiration policies have limited benefits as users typically do not make significant changes to their passwords. Companies could enforce rules that require larger

changes and check for certain modifications, but this would have negative usability outcomes. Password expiration policies are most beneficial to account security if passwords are sufficiently random [31]. As people are unlikely to create and maintain random passwords on their own, organizations should consider the use of password managers with built-in generators, especially since some major password managers have enterprise versions of their software [21]. In our study, we found that those who did use a generator to create their password were much more likely to use one to update it and store their password in a password manager. However, it should be noted that many organizations that have implemented password expiration also have other policies which indirectly prevent their employees from using password managers. For example, some organizations in the United States government prevent employees from installing non-approved software, or even storing passwords on their terminals [2,35]. Considering our findings, such policies likely diminish any security benefit of having an expiration policy.

Across both surveys, we observed that participants strongly felt that password changes were important for account security. Some participants revealed that they held this perception because they trust the IT staff at their organizations and that is the advice they are repeatedly told. Overall, we observed that users adapt to the demands placed on them, even if in undesirable ways. This result may bode well for the future as security recommendations and best practices change with technology.

6. ACKNOWLEDGMENTS

This research was supported by the North Atlantic Treaty Organization (NATO) through Carnegie Mellon CyLab. This work was also supported in part by the CyLab Presidential Fellowship. The authors would like to thank Jessica Colnago for her contributions toward our preliminary analysis, and reviewers for their feedback.

7. REFERENCES

[1] S. Bellovin. Unconventional wisdoms. *IEEE Security and Privacy*, 4(1):88, 2006.

[2] Centers for Medicare and Medicaid Services. CMS policy for the acceptable use of CMS desktop/laptop and other it resources. `https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity`, December 2008.

[3] S. Chiasson and P. C. van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 77(2-3):401–408, 2015.

[4] Y.-Y. Choong, M. Theofanos, and H.-K. Liu. NISTIR 7991: United states federal employees' password management behaviors - a department of commerce case study. Technical report, National Institute of Standards and Technology NIST, March 2014.

[5] Communications-Electronics Security Group. The problems with forcing regular password expiry. `https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry`, 2016.

[6] L. Cranor. Time to rethink mandatory password changes. `https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes`, March 2016.

[7] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, volume 14, pages 23–26, 2014.

[8] M. Farcasin and E. Chan-tin. Why we hate IT: Two surveys on pre-generated and expiring passwords in an academic setting. *Security and Communication Networks*, 8(13):2361–2373, 2015.

[9] D. Florêncio and C. Herley. A large-scale study of web password habits. In *Proceedings of the International Conference on World Wide Web (WWW)*, pages 657–666, 2007.

[10] D. Florêncio and C. Herley. Where do security policies come from? In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 10:1–10:14, 2010.

[11] S. Gaw and E. W. Felten. Password management strategies for online accounts. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 44–55, 2006.

[12] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos. NIST Special Publication 800-63b: Digital Identity Guidelines. Technical report, National Institute of Standards and Technology NIST, 2017.

[13] B. Grawemeyer and H. Johnson. Using and managing multiple passwords: A week to a view. *Interacting with Computers*, 23(3):256–267, 2011.

[14] P. G. Inglesant and M. A. Sasse. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392, 2010.

[15] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). Information technology: Security techniques, code of practice for information security management: ISO-IEC 27002:2013, October 2013.

[16] I. Ion, R. Reeder, and S. Consolvo. "No one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 327–346, 2015.

[17] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of Mechanical Turk workers and the US public. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 37–49, 2014.

[18] A. Kittur, E. H. Chi, and B. Suh. Crowdsourcing user studies with Mechanical Turk. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 453–456, 2008.

[19] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134, 2017.

[20] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2595–2604, 2011.

[21] LastPass. Lastpass enterprise. https://www.lastpass.com/enterprise, February 2018.

[22] D. Malone and K. Maher. Investigating the distribution of password choices. In *Proceedings of the International Conference on World Wide Web (WWW)*, pages 301–310, 2012.

[23] K. Muller. Statistical power analysis for the behavioral sciences. *Tehcnometrics*, 31:499–500, 1989.

[24] National Cyber Security Centre. Password guidance: Simplifying your approach. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach, August 2016.

[25] G. Notoatmodjo and C. Thomborson. Passwords and perceptions. In *Proceedings of the Australasian Conference on Information Security (ACISP)*, pages 71–78, 2009.

[26] PCI Security Standards Council. Payment card industry (PCI) data security standard.

[27] S. Pearman, J. Thomas, P. Emani Naeini, H. Habib, L. Bauer, N. Christin, L. Faith Cranor, S. Egelman, and A. Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, 2017.

[28] S. Riley. Password security: What users know and what they actually do. *Usability News*, 8(1):2833–2836, 2006.

[29] B. Schneier. Security of password managers. https://www.schneier.com/blog/archives/2014/09/, September 2014.

[30] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, page 2, 2010.

[31] E. Spafford. Security myths and passwords. http://www.cerias.purdue.edu/site/blog/post/password-change-myths/, April 2006.

[32] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[33] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. Do users' perceptions of password security match reality? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3748–3760, 2016.

[34] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. I Added '!' at the End to Make It Secure: Observing Password Creation in the Lab. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[35] U.S. Immigration and Customs Enforcement. General rules of behavior for users of DHS systems and IT resources that access, store, receive, or transmit sensitive information. https://www.ice.gov/doclib/sevis/pdf/behavior-rules.pdf, April 2008.

[36] A. J. Viera, J. M. Garrett, et al. Understanding interobserver agreement: The kappa statistic. *Fam Med*, 37(5):360–363, 2005.

[37] E. von Zezschwitz, A. De Luca, and H. Hussmann. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Proceedings of the IFIP Conference on Human-Computer Interaction*, pages 460–467. Springer, 2013.

[38] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, pages 162–175. ACM, 2010.

[39] Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, pages 176–186, 2010.

[40] L. Zhang-Kennedy, S. Chiasson, and P. C. van Oorschot. Revisiting password rules: Facilitating human management of passwords. In *Proceedings of the APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–10, 2016.

APPENDIX

A. SCREENING SURVEY

1. How many workplace passwords do you have? *
   - 0
   - 1
   - 2
   - ...
   - 7
   - 8 or more
2. How many of your workplace passwords are you required to regularly change (i.e., they have an expiration policy)?*
   - All of my workplace passwords
   - Most of my workplace passwords
   - Some of my workplace passwords
   - None of my workplace passwords
   - Not sure
3. How old are you? *
   - 18-24 years old
   - 25-34 years old
   - 35-44 years old
   - 45-54 years old
   - 55-64 years old
   - 65-74 years old
   - 75 years or older
   - I prefer not to answer
4. What is your gender? *
   - Male
   - Female
   - Other (please specify)
   - I prefer not to answer
5. What is your race/ethnicity? *
   - American Indian or Alaska Native

- Asian
- Black or African American
- White/ Caucasian
- Hispanic or Latino
- Non Hispanic
- Other
- I prefer not to answer

6. Which of the following best describes your highest achieved education level?*
   - Some High School
   - High School Graduate
   - Some college, no degree
   - Associates degree
   - Bachelors degree
   - Graduate degree (Masters, Doctorate, etc.)
   - Other
   - I prefer not to answer
7. Which of the following best describes your primary occupation? *
   - Administrative Support (e.g., secretary, assistant)
   - Art, Writing, or Journalism (e.g., author, reporter, sculptor)
   - Business, Management, or Financial (e.g., manager, accountant, banker)
   - Education or Science (e.g., teacher, professor, scientist)
   - Legal (e.g., lawyer, paralegal)
   - Medical (e.g., doctor, nurse, dentist)
   - Computer Engineering or IT Professional (e.g., programmer, IT consultant)
   - Engineer in other field (e.g., civil or bio engineer)
   - Service (e.g., retail clerk, server)
   - Skilled Labor (e.g., electrician, plumber, carpenter)
   - Unemployed
   - Retired
   - College student
   - Graduate student
   - Mechanical Turk worker
   - I prefer not to answer

B. WORKPLACE PASSWORDS SURVEY

The next few questions will ask you about your main workplace password. Please keep the following in mind:

- If you have more than one workplace, please respond using the workplace you consider to be your main workplace.
- If you have more than one password at your main workplace, respond using the one you consider to be your main password.
- If you are a student you may consider your university to be your main workplace.
- If Mechanical Turk is your main workplace, you should consider your Mechanical Turk password as your main workplace password.

1. How many workplace passwords do you have?
   - none
   - 1
   - 2
   - ...
   - 7
   - 8 or more
2. Thinking back to when you first created your main workplace password, which of the following methods did you use?
   - ☐ Used the first letter of each word in a phrase
   - ☐ Used the name of someone or something
   - ☐ Used a word in English
   - ☐ Used a word in a language other than English
   - ☐ Added numbers to the beginning or end of a word or name
   - ☐ Added symbols to the beginning or end of a word or name
   - ☐ Substituted symbols for some of the letters in a word or name (e.g. '@' instead of 'a')
   - ☐ Substituted numbers for some of the letters in a word or name (e.g. '3' instead of 'e')
   - ☐ Removed letters from a word or name
   - ☐ Used a phone number
   - ☐ Used an address
   - ☐ Used a birthday
   - ☐ Reused a password from another account exactly
   - ☐ Reused a password from another account with some modifications
   - ☐ Used something else (please specify)
   - ☐ I prefer not to answer
3. How many of your workplace passwords are you required to regularly change, i.e. they have an expiration policy?
   - All of my workplace passwords
   - Most of my workplace passwords
   - Some of my workplace passwords
   - None of my workplace passwords
   - Not sure
4. How often are you required to change your main workplace password?
   - Every week
   - Every 30 days
   - Every 60 days
   - Every 90 days
   - Every year
   - Never
   - Not sure
   - Other (please specify)
5. Some organizations require their employees to change their passwords every 60 days. What do you think the impact of this policy is on security compared to organizations that do not require their employees to change their passwords at all?

- ○ It makes it less likely that an unauthorized person will log in to my account
- ○ It makes it more likely that an unauthorized person will log in to my
- ○ account
- ○ It doesn't impact security
- ○ I don't know

6. Why do you think this is the impact?
7. What do you think is the main reason for a workplace to set an expiration date on their employees' main passwords?
8. How often do you think your workplace should require its employees to change their main workplace password?
   - ○ Every week
   - ○ Every 30 days
   - ○ Every 60 days
   - ○ Every 90 days
   - ○ Every year
   - ○ Never
   - ○ Not sure
   - ○ Other (please specify)
9. Why do you think your workplace should require its employees to change their main password with this frequency?
10. The last time you changed your main workplace password, what approaches did you use? (select all that apply)
    - □ Adding a date (e.g. "raven" →"raven2016")
    - □ Adding a sequence (e.g. "dance#7" →"dance#789")
    - □ Capitalizing a character (e.g. "candy#" →"candY#")
    - □ Deleting digits/special characters (e.g. "alex28!!!" →"alex28!!")
    - □ Duplicating digits/special characters (e.g. "1!" →"11!")
    - □ Incrementing a character (e.g. "dance#7" →"dance#8")
    - □ Moving a letter, digit or special character block (e.g. "$steve27" →"27$steve")
    - □ Substituting digits/special characters with the same character type (e.g. "tar!heel1" →"tar!heel4")
    - □ Substituting letters with matching characters (e.g. "raven" →"r@ven")
    - □ Substituting digits or special characters with the "shift" character for the same key (e.g. "l00py*!2" →"l00py*!@")
    - □ Changing a small part of the previous password in a way not mentioned
    - □ Creating a completely new password
    - □ Reusing old passwords from other accounts
    - □ Using a password generator
    - □ Using a different approach (please specify)
    - □ I don't change my workplace password
11. How often have you used your strategy to change your main workplace password when it expired?
    - ○ I only changed my password once
    - ○ a couple of times (not often)
    - ○ most of the time
    - ○ every time
    - ○ I never changed my password
    - ○ other (please specify)
12. Why do you change your password this way? (select all that apply)
    - □ I have always done it this way
    - □ I heard about it from someone
    - □ I read it somewhere
    - □ I think it makes the password easier to remember
    - □ I think it makes the password stronger
    - □ It was the first strategy I thought of
    - □ other (please specify)
13. When changing your workplace password because the old one expired, do you always use the same strategy?
    - ○ I use the same strategy every time
    - ○ I use slightly different strategies at different times
    - ○ I use very different strategies at different times
14. How similar is your main workplace password to a password you use for another account at your workplace?
    - ○ My main workplace password is identical to a password I use for another workplace account
    - ○ My main workplace password is similar to a password I use for another workplace account
    - ○ My main workplace password is very different from any passwords I use for other workplace accounts
    - ○ I only have one workplace password
15. How similar is your main workplace password to a password you use for a non-workplace account?
    - ○ My main workplace password is identical to a password I use for a nonworkplace account
    - ○ My main workplace password is similar to a password I use for a nonworkplace account
    - ○ My main workplace password is very different from any passwords I use for non-workplace accounts
16. Where did you learn about changing your password this way? (select all that apply)
    - □ Boss
    - □ Colleague
    - □ Family member
    - □ Friend
    - □ IT department
    - □ Internet
    - □ Other (please specify)
17. When I last changed my main workplace password because it had expired, my new password was:
    - ○ Much weaker
    - ○ Weaker
    - ○ About the same
    - ○ Stronger
    - ○ Much stronger
    - ○ I don't know
18. How many workplace passwords do you have?
    - ○ none
    - ○ 1

- 2
- ...
- 7
- 8 or more

19. Frequent password expiration makes it less likely that an unauthorized person will break into my account.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
20. I find having to change my password due to my workplace expiration policy **difficult**.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
21. I find having to change my password due to my workplace expiration policy **easy**.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
22. Frequent password expiration makes it less likely that an unauthorized person will break into my account.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
23. I find having to change my password due to my workplace expiration policy **difficult**.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
24. I find having to change my password due to my workplace expiration policy **easy**.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
25. I find having to change my password due to my workplace expiration policy **annoying**.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
26. I find having to change my password due to my workplace expiration policy **fun**.
    - Strongly Disagree
    - Disagree
    - Neutral
    - Agree
    - Strongly Agree
    - Not applicable
27. What do you do to help yourself remember your main workplace password?
    - ☐ I let my web browser store it
    - ☐ I store it in an encrypted file
    - ☐ I store it in a password manager
    - ☐ I store it on a computer or device protected with another password
    - ☐ I store it on a computer or device that only I use
    - ☐ I write down my password on a piece of paper
    - ☐ I write down a reminder instead of the actual password
    - ☐ Nothing, I memorize it
    - ☐ I prefer not to answer
    - ☐ Other (please specify)
28. Why do you use this strategy to remember your main workplace password?
29. How many logins does it take for you to memorize your main workplace password?
    - 1-2 logins
    - 3-5 logins
    - 6-10 logins
    - More than 10 logins
    - None, I memorize it when I create it or use a password I already memorized
    - I don't memorize my main workplace password
30. How many times have you been unable to log into your main workplace account in the past year due to not having your password? (e.g. you forgot your password, the password was stored in a different device, etc.)
    - Never
    - 1-2 times
    - 3-5 times
    - 6-10 times
    - More than 10 times
31. What do you need to do to change or recover your main workplace password if you forget it? (select all that apply)
    - ☐ I call someone on the phone
    - ☐ I send someone an email
    - ☐ I physically go somewhere or see someone in person
    - ☐ I mail someone a letter

- ☐ I use a website
- ☐ I don't know
- ☐ Other (please specify)

32. Who or what reminds you in advance of your password expiring to change your main workplace password? (select all that apply)
    - ☐ Boss
    - ☐ Colleague
    - ☐ IT department
    - ☐ Automated e-mails
    - ☐ Software on my computer
    - ☐ I don't get reminders in advance
    - ☐ Other (please specify)
33. When do you get the first reminder to change your main workplace password before it expires?
    - ○ Less than 1 day in advance
    - ○ 1 day in advance
    - ○ Less than a week in advance
    - ○ 1-2 weeks in advance
    - ○ 3-4 weeks in advance
    - ○ 1 month in advance
    - ○ More than 1 month in advance
    - ○ Other (please specify)
34. How does the reminder impact your effort in changing your main workplace password?
    - ○ I put more effort in updating my password
    - ○ I put less effort in updating my password
    - ○ It doesn't, I put the same amount of effort
    - ○ Other (please specify)
35. Has your main workplace password ever been accidentally leaked or otherwise compromised?
    - ○ Yes, I lost the device which had the password stored and the device was not password protected
    - ○ Yes, I lost the paper on which I wrote my password
    - ○ Yes, someone guessed it
    - ○ Yes, someone watched me type it in
    - ○ Yes, the IT infrastructure was breached
    - ○ Yes, other
    - ○ No
    - ○ Not sure
36. What did you do when your password was leaked? (select all that apply)
    - ☐ I changed my password before it expired
    - ☐ I kept my password and waited for it to expire to change it
    - ☐ I learned how to create stronger passwords
    - ☐ I changed where I stored my password
    - ☐ Other (please specify)
37. Do you have any other comments about your workplace password or its expiration policy? (optional)
38. Questions 38-42 are the same as Q3-7 in the screening survey above

C. PASSWORD PERCEPTIONS SURVEY

1. Questions 1-4 are the same as Q3-7 in the screening survey above
5. Have you ever held a job or received a degree in computer science or any related technology field?
    - ○ Yes
    - ○ No
6. Are you either a computer security professional or a student studying computer security?
    - ○ Yes
    - ○ No
7. To keep your account secure, how important is it to use a complex password (e.g., a long password with digits, symbols, and capital letters)? *
    - ○ 1 (Not important)
    - ○ ...
    - ○ 5 (Very important)
8. Please explain your answer to the question above. *
9. To keep your account secure, how important is it to store your password in a safe place (e.g, on a note hidden out of sight of other people) or not store it at all? *
    - ○ 1 (Not important)
    - ○ ...
    - ○ 5 (Very important)
10. Please explain your answer to the question above. *
11. To keep your account secure, how important is it to change your password periodically? *
    - ○ 1 (Not important)
    - ○ ...
    - ○ 5 (Very important)
12. Please explain your answer to the question above. *
13. To keep your account secure, how important is it to create a password that you do not already use somewhere else? *
    - ○ 1 (Not important)
    - ○ ...
    - ○ 5 (Very important)
14. Please explain your answer to the question above. *
15. Please rank the following in their order of their harm to account security, with "1" being the most harmful. (Multiple options may have the same ranking) *
    - Creating a password you have already used somewhere else (either exactly or with small modifications)
    - Storing the password in a place where others can access it
    - Not changing the password periodically
    - Creating a simple password (e.g., with no symbols or digits)
16. For each pair, which do you think contributes more to account security? * [Answered as "Left contributes much more," "Left contributes slightly more," "Both contribute equally," "Right contributes slightly more," "Right contributes much more"]

- Using a complex password | Storing your password in a safe place or not storing it at all
- Using a complex password | Creating a password that you do not already use somewhere else
- Using a complex password | Changing your password periodically
- Changing your password periodically | Creating a password that you do not already use somewhere else
- Storing your password in a safe place or not storing it at all | Changing your password periodically
- Storing your password in a safe place or not storing it at all | Creating a password that you do not already use somewhere else

17. How many workplace passwords do you have in total? *
    - ○ 0
    - ○ 1
    - ○ 2
    - ○ ...
    - ○ 7
    - ○ 8 or more

    Logic: The following two questions are hidden if "How many workplace passwords do you have in total?" is "none"

18. What do you do to help yourself remember your main workplace password? *
    - ☐ Let your web browser store it
    - ☐ Store it in an encrypted file
    - ☐ Store it in a password manager
    - ☐ Store it on a computer or device protected with another password
    - ☐ Store it on a computer or device that only you use
    - ☐ Write it down on a piece of paper
    - ☐ Write down a reminder instead of the actual password
    - ☐ Nothing, you memorize it
    - ☐ Prefer not to answer
    - ☐ Other (please specify)

19. Does your workplace have an expiration policy for your main password? *
    - ○ Yes
    - ○ No

    Logic: The following questions five are hidden if "Does your workplace have an expiration policy for your main password?" is "No" or "Not Sure"

20. How often are you required to change your main workplace password? *
    - ○ Every week
    - ○ Every 30 days
    - ○ Every 60 days
    - ○ Every 90 days
    - ○ Every year
    - ○ Never
    - ○ Not sure
    - ○ Other (please specify)

21. Suppose your workplace's expiration policy changed and your main workplace account password will no longer expire. How likely would you be to continue to periodically change the password of your account anyways? *
    - ○ Very unlikely
    - ○ Unlikely
    - ○ Neither likely or unlikely
    - ○ Likely
    - ○ Very likely

22. Please explain your answer to the question above. *

23. Suppose your workplace's expiration policy changed and your main workplace account password will no longer expire. Going forward, how would you remember your main workplace password? *
    - ☐ Let your web browser store it
    - ☐ Store it in an encrypted file
    - ☐ Store it in a password manager
    - ☐ Store it on a computer or device protected with another password
    - ☐ Store it on a computer or device that only you use
    - ☐ Write it down on a piece of paper
    - ☐ Write down a reminder instead of the actual password
    - ☐ Nothing, you would memorize it
    - ☐ Prefer not to answer
    - ☐ Other (please specify)

24. Suppose your workplace's expiration policy changed and your main workplace account password will no longer expire. Going forward, would you be more or less likely to do the following? * [Answered on a 5-point Likert scale from "Much more likely" to "Much less likely"]
    - Use a complex password
    - Create a password you do not already use somewhere else

    Logic: The following questions five are hidden if "Does your workplace have an expiration policy for your main password?" is "Yes"

25. How often do you change the password of your main workplace account? *
    - ○ Never
    - ○ Every week
    - ○ Every month
    - ○ Every few months
    - ○ Every year
    - ○ Other (Please specify)

26. Please explain why you change your password with the frequency indicated above. *

27. Suppose your workplace implemented an expiration policy and from now on your main workplace account password will expire periodically. Going forward, how would you remember your main workplace password? *
    - ☐ Let your web browser store it
    - ☐ Store it in an encrypted file
    - ☐ Store it in a password manager

- ☐ Store it on a computer or device protected with another password
- ☐ Store it on a computer or device that only you use
- ☐ Write it down on a piece of paper
- ☐ Write down a reminder instead of the actual password
- ☐ Nothing, you would memorize it
- ☐ Prefer not to answer
- ☐ Other (please specify)

28. Suppose your workplace implemented an expiration policy and from now on your main workplace account password will expire periodically. Going forward, would you be more or less likely to do the following? * [Answered on a 5-point Likert scale from "Much more likely" to "Much less likely"]
    - Use a complex password
    - Create a password you do not already use somewhere else