USENIX Symposium on Usable Privacy and Security (SOUPS) 2019. August 11 -- 13, 2019, Santa Clara, CA, USA.

.

Password Expiration Policy: Focusing on Students

Daniel Browning, *Contributor* Jay Dave, *Contributor*
Vianca Barlis, *Contributor* Carson Bannister, *Contributor* Xavier Esquilin, *Contributor*

Abstract

Policies that require students to update their passwords regularly have become common at universities. 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 Google Forms through which we examined people's self-reported behaviors in using and updating school passwords, and their attitudes toward four previously studied password-management behaviors, including periodic password changes. Our findings show that 78.6% of our participants believe they should be required to change their university password two times a year. This corresponds with the 66.7% of participants who change their password at least one time per year. When faced with being inconvenienced, participants seem to understand that security of their account is more important. When it comes time to change the password on their main account, 57.1% of our participants indicated that they modify their existing password to fix the requirements. This is done to help with memorization as 60% of participants indicated that this is their main form of retaining passwords. We also found that a majority of our participants understood the importance in security as 66.7% indicated that storing a password in a place others can access it i.e on a sticky note was most harmful.

1. Introduction

Passwords are vital in life today. They secure some of our most precious information, and even sometimes our houses. Being so vital, they require maintenance, mostly in the form of changing them. Changing passwords is meant to keep them secure: by changing the password, it supposedly not only prevents reuse, but it prevents people from guessing or even brute forcing your password. This is all an ideal scenario, and oftentimes, like we see in other cases, humans are the weakest link in the chain of security. In this case, we may sometimes change our passwords improperly and against guidelines set by the organization. Improperly changing a password can mean reusing the same password, only slightly changing it, using a completely new, not-as-secure password.

To combat the human weakness of passwords, expiration policies were created. These policies meant it was required to change a password after a certain amount of time had passed, and then the cycle would repeat. Some have openly accepted these policies as being necessary for password security, but others have spoken out against them, saying it only creates trouble and causes less secure passwords.

1.1. Goals

The goal of this research study is to examine the effectiveness of password expiration policies and to determine if password expiration policies produce more harm than good or more good than harm. It is to expand upon the original study to more closely examine college students and the password expiration policies universities implement.

1.2. Original Study

The original study was presented in 2018, and it sought to better understand the effectiveness, benefits, and even harms that password expiration policies could cause. Given the common practice of expiration policies as well as the prior work to the study suggesting these policies cause more harm than good, the creators saw the need for further understanding. Password expiration policies are policies that require users (employees in the case of the original study) to change their passwords in a determined frequency (three months, semi-annually, annually, etc.) to supposedly increase security, as it makes any password compromises insignificant because the password will be changed. It also makes brute force attacks nearly impossible, as the password is ever changing, and this all assumes a new, secure password is chosen, so the time to break it is quite long.

1.2.1. Original Study Methodology

In the original study, the creators utilized Mechanical Turk, creating two different surveys which they would then recruit users from Mechanical Turk to participate in said surveys. The first survey consisted of questions related to the users' actual practices related to changing their passwords in accordance with their employers' password expiration policies or just when changing them in general. A total of 407 people finished the full password practices survey, and 339 completed and qualified for use in the password perceptions survey. Both qualitative and quantitative data analysis were performed on the results of the surveys, as some of the questions were open ended and some were multiple choice/select all.

1.2.2. Original Study Results

The results of the original study were not polarizing or shocking in any way. In the original findings, they found data suggesting that the previously considered effects of password expiration policies, both positive and negative, are not accurate. For example, they found that due to password expiration policies, most users would not resort to behaviors that would greatly compromise security. However, when they did change their passwords, the data suggested that the new passwords were not any stronger than the ones being replaced. It was also found that password expiration policies were reported to hold a significant role in security, according to users' perceptions. This significance was not greater than that of other, more thoroughly proven methods of security enhancement, however. The data also suggested that, despite a lack of evidence to support it, the repetition of security and privacy advice or guidelines is beneficial, as it causes users to internalize it.

1.2.3. Original Study Limitations

The original study did have its limitations; for example, users of Mechanical Turk are reported to have increased privacy concerns and a higher level of privacy literacy than most people, but that was reasonably disregarded, as other results have shown that Mechanical Turk is still a quite reliable source for diverse information from human subjects.

1.2.4. Original Study Summary

The main take-aways from the study are the demand for study: given the results of previous studies and the common acceptances that were not proven, there is a demand for further study. Additionally, there has been a pattern shown in other studies as well highlighting the need for more education and better education for users when it comes to security and privacy.

2. Related Work

There are quite a few other studies that have examined password expiration policies, including the original study we have adapted to fit our needs. Our research differs from them in the same way the original did: it examines the strategies used when changing a password under the expiration policy as well as the overall perception of the password policy. We have examined the related work in the original study to find the best fit related work to our own study, given they are so similar.

A self-reporting diary study was conducted by Grawemeyer and Johnson, and it observed that the average of their participants logged into various accounts over forty five times per one week [1]. Work-related activities accounted for forty three percent of all logins in their sample, which highlights the importance of the original study, which in turn highlights the importance of our own study, as it is the same, only it focuses directly on college students.

We have also seen that there are oftentimes patterns and strategies for changing passwords that make it easier for people to choose a "new" one [2,3]. Unfortunately for security, there has been great evidence that the main strategy for changing passwords and selecting them is to reuse other passwords in some form [2,3,4,5,6]. There has been direct correlation to suggest that the more passwords a user has, the more they are likely to reuse passwords in some form [7]. In addition to this, it has also been observed in studies that people generally attempt to match the security of the password with the significance of the account [3,8]. For example, for a magazine or forum account, the password may not be very secure, but they will try and make their financial passwords and social media passwords secure. That in itself shows most users are already aware of the "usability vs. security" tradeoff debate. It was also seen during an interview study that most users do not change their passwords unless required to or prompted to [2].

Indeed, every user is different in some way, but there is evidence to show that most users rely on memory to recall their passwords [1,7,9].

2.1. Password Expiration Difficulties

In examining password expiration issues and policies, there have been multiple studies, including one that examined seventy five websites and their policies and found ten percent required them to change their passwords regularly. One of the largest difficulties seen was that in a study which showed only thirty percent of the participants created a completely new password when compelled to change their university password and nineteen percent had issues recalling their new password which they had created [11].

Some other issues that have arisen are being reminded to change a password too early, having trouble keeping track of updated passwords, difficulty creating passwords that meet the institution's password requirements, and fear of being locked out of an account due to wrong passwords [12,13].

Password cracking attacks are quite effective against people who do not properly secure their passwords when they update them, meaning they make predictable changes to their passwords like adding an "!" to the end or capitalizing a letter of a word [14]. There was also a study done that furthered the case against password policies, demonstrating that with the capabilities of computers these days, it is no longer reasonable to assume that changing passwords is faster than potentially cracking them [15].

3. Methodology

We conducted a three part survey on Google Forms through which we examined people's self-reported behaviors in using and updating school passwords, and their attitudes toward four previously studied password-management behaviors, including periodic password changes. We also asked them about what strategies they used during these password changes to better gauge how secure their new passwords were in comparison with their old ones. We used **ONLY** quantitative data analysis for our study.

3.1. Data Collection

In examining password expiration issues and policies, there have been multiple studies, including the one we originally based ours off. We used almost the same technique for gathering data and the survey itself. We used almost identically the same survey, with some modifications, and we made it one, three part survey, rather than the original multiple surveys. We also used Google Forms rather than Mechanical Turk.

3.2. Password Survey

Our only survey was a combination of the original surveys into one, with modifications of course. We felt it more efficient to do this in order to both screen and collect useful data at the same time. In order to ensure accurate results from university students, the results were restricted to only be from .uncc.edu email addresses.

Our survey has forty five questions, from radio buttons to multiple checkboxes, but they are all quantitative results and would be subject to quantitative analysis. The survey was designed to gain a better understanding of perceptions related to university level password expiration policies as well as the strategies students use when dealing with these policies. The survey examines the perception of expiration policies as well as what specific things students do to change their passwords, if they change them, when they think they should change them, and what changing them actually does. It also examines what they perceive as more important for security.

We had a total of twelve responses for our pilot study, an adequate number to gauge the effectiveness of our own study methods. Participants were volunteers, being compensated by gratitude. The survey will be attached to the appendix.

3.3. Data Analysis

In our analysis of the results, we made sure there were no fraudulent reponses to our survey, and we saw a consistent quality of answers. We used only quantitative data analysis, given all the questions were some form of multiple choice and were not open to interpretation or free response, other than the option for "other: please specify," which we did not get any of. We used visual representations of data and automated data categorizing to analyze our data for our purposes, which is to examine the perceptions of password expiration policies for students as well as the strategies used by students when encountering these policies.

3.4. Limitations

Our study does have its limitations; first and foremost of these limitations is that it is self-reported, and self-report studies are unfortunately prone to bias from participants. We have tried to combat this by making it low-pressure, anonymous, and simple, so that way individuals may be less prone to provide incorrect information. Additionally, another limitation is that it is only for college students at our university (so far), so there is a lack of representation from the whole population. We also noticed there were only 18-24 year olds responding, so age may also provide a bias in our data set.

4. Results

Our results include questions about how students create, update and manage their student account passwords as well as other daily usage passwords. We have collected and analyzed dad collected from 29 students at The University of North Carolina at Charlotte.

4.1 Password Expiration Policies

75.9% of our population stated that when users are required to change their password every 60 days that this makes it less likely that an unauthorized person will login to their account. The participants were then asked how often a password should be changed by requirement of the university. Out of our results, 37.9% of our population stated that passwords should be changed twice a year, 34.5% of our population stated that passwords should be changed every year, 13.8% of our population stated that passwords should be changed never or every 30 days.

4.2 Password Creation and Reuse

When creating a new password the most common approaches (24.1%) were capitalizing a letter, Creating a completely new password or reusing an old password from another account. Duplicating digits/special characters or changing a small part of a previous password was a close second to these strategies and 24.1% of our population reported using them. With these tendencies, 37.9% uses these strategies every time, 37.9% use these most of the time, and 24.1% use these a couple of times (not often).

When asking the participants why they change their passwords the way that they do the most common response was "I think it makes the password easier to remember" followed by "it was the first strategy I thought of".

When asked about the similarity of school passwords to another account at school, 24.1% reported main password being very different from any passwords they used on other accounts, 24.1% reported that their password is identical to a password they use for another account, and 51.7% reported that their password is similar to a password they use for another account.

When asked about the similarity of school password to a password used for a non-school account, 37.9% reported that their main password is very different from any passwords they use for non-school accounts, 44.8% reported that their main school password is similar to a password they use for a non-school account, and 37.9% stated that their main password is identical to a password they use for a non-school account.

When asked about the last time that the participant changed their password due to an expiration 75.9% stated that their password was about the same with the remaining population stating that it was stronger or they did not know.

62.1% of our population felt that frequent password expirations makes it less likely that an unauthorized person will break into their account. The remainder of the population felt either neutral or disagreed.

When asked about the level of difficulty that is experienced when having to change their passwords due expiration policies, 48.3% stated that they do not find it difficult. 37.9% felt indifferent and only 13.8% found it difficult to change their passwords.

4.3 Password Recall and Lockouts

Our participants gave insight into how they go about recalling their passwords. The most common recall strategy in the survey was by attempting to memorize the password (58.6%). In the password perception survey, 65.5% of users stated they utilize memorization as opposed to writing the password down.

While a majority of participants recorded memorizing their password, 68.9% of users reported storing their password in a password manager. While in the password perception survey 13.8% believe storing your password in a safe place is more important for account security.

The participants were asked to recall the number of times that they were unable to log in to their main academic account due to forgetting their password in the past year. 27.6% of responses stated they forgot the password three to five times and 37.9% forgot their password one-two times.

4.4 Password Update Behavior

When asked what strategies our participants used when updating their password 24.1% stated that they capitalized a character from their old password. Another 10.3% stated that they modify their password by moving characters around, and 6.9% stated that they substitute letters with matching symbols.

When asked whether they use the same strategy when changing passwords, 37.9% stated that they keep using the same strategy every time while the other 24.1.1% modify their strategy at different times.

4.5 Security Perceptions

Only 31% find it very important to store passwords in a safe place or not store it at all. 58.6% find it important, while 10.3% are unconcerned about storing their passwords. More than half of the participants (58.6%) find it very harmful(1) to store their passwords where others can access it. 24.1% participants agree at level 2 of harmfulness and 6.9% are indifferent at level 3.

When asked if properly storing passwords or changing passwords periodically is more important, more responded to storage to be better. However, 58.6% find both to be important. 34.5% of the participants are indifferent about changing their passwords periodically and 6.8% find it not important.

When asked if changing passwords periodically or not reusing passwords is more secure, 17.2% says that changing passwords periodically is more effective. While 51.7% say that both are equally important.

When asked how often participants change their passwords, 20.7% say never. While 41.4% say after every few months. 27.6% say every year, and 3.4% say when they are asked to.

When told that their main account password will no longer expire, they were asked how to remember it. 65.5% of the participants said they will remember it, 27.6% says that they will store it on their personal device, 31% says that they will let their web browser store it, 24.1% says that they will store it in a password manager, and 27.6% says they will store it in their device protected by another password.

Half of the participants say that it is important to not reuse passwords. While 35.7% are indifferent about the subject.

Half of the participants find it risky to reuse their passwords from other accounts.

41.4% voted 3 (neither harmful nor helpful) if they reused their passwords in other accounts. However, 10.3% says that it is very risky.

Most people say that creating a password with no symbols or numbers are important.

We find that 50% of the participants find usage of complex passwords to be important, plus 14.3% find it very important.

When asked whether using a complex password is more important than creating a password not already used anywhere else, participants of 50% say that both are important.

When asked whether using a complex password is more important than properly storing passwords, 35.7% of participants find it both to contribute more to account security. However, another 35.7% of participants find using complex passwords to be more effective.

Most people say that using complex passwords is more important than changing passwords periodically.

5. Discussion

Overall, our survey results were quite on-par with what we have seen before in the original study. This was not a surprise, as it was simply an adaptation to the original study, as we expected to see similar results. In our study, we saw the practices the participants used when changing passwords were similar to those used in the original study, meaning the new passwords being created by the policies were almost never more secure than the ones they were replacing. For example, many users stated they reuse another password or make a simple change to an existing one in order to create a new password when their password is going to expire. This simplicity can be attributed to the convenience of doing it this way, as many of our participants said they used a certain method because it made it easier to remember the password later. Additionally, there was a majority of participants who said their school password was very similar to another password for another school account, which is in line with the original study as well as previous work examining password reuse. There was surprisingly an almost even split of participants who reported using a very different password for other, non-school accounts. It was also notable that only a small percentage of participants found changing their password frequently in accordance with a password expiration policy is difficult, while the others were indifferent or did not find it difficult at all. This highlights the findings of the original study, showing that the negative effects and perceptions of password expiration policies are not accurate or are exaggerated in some way.

Our results showed a clear method to password recall, that our participants generally just tried to memorize their passwords. To supplement this, however, it was found that most users did in fact use some sort of password manager or automated password storage to keep the password secure. Again, this can be attributed possibly to convenience, as storing passwords in a manager can be complex and it involves utilizing a manager, while memorizing can be much easier, when it works. Again, this highlights our theme that has persisted throughout academia in privacy and security related concerns, and that is of course that humans are the weakest link in privacy. As a consequence of this, we have also seen that a majority of participants were unable to log into their account as a result of forgetting or losing their password.

In our perceptions section of the survey, it was made clear that a majority of participants agree that password storage is vital to security, which correlates to not storing a password in a location others might see it or be able to view it. Much like the original study, we also saw a clear majority in storage vs. frequency of change, showing that participants clearly perceived storing passwords securely is more important to privacy and security than changing a password frequently, but both are important. Participants also reported that changing passwords and not reusing passwords are almost equally effective. The self-reported frequency of passwords being changed is also interesting, as it shows almost a majority of participants change it every few months, but a fifth of participants said they do not ever change some passwords, which highlights a security concern that we have seen before. Given a hypothetical of their main password no longer expiring, a majority of participants said they would keep track of it simply by remembering it, without the use of any external help. This, coupled with the reporting of forgetting or getting locked out of an account, could be worrisome, as it shows participants may have an inflated sense of their own abilities to remember their passwords, which could pose a security risk, as they may opt then for less secure passwords in order to remember them, or they may store it in more locations, possibly in less secure locations.

We found a generally even split between what is more important to security, which shows that users are aware that there is not just one trick to stay secure, rather it is the combination of practices that leads to safety. This, if it can be educated, could help bridge the gap of human-error that causes so many privacy and security related concerns. This is in line with our original study, but it veers slightly away in this case, but it could be possibly attributed to having a greater privacy concern or even more than that, a higher level of technical literacy.

6. Conclusion

In summary, our study was much like the original, though unfortunately not as large. It showed a similar data analysis, even without the qualitative analysis that was performed in the original study. In our quantitative analysis we saw similar results, showing not only were the positive effects of password expiration policies perhaps not as severe, but the negative ones too. With this information, we can recommend further study and perhaps usability testing on alternative methods for providing password or authentication security. Our results signify the pattern that exists throughout security: humans are the most insecure piece of the puzzle of security. They are not the glue, rather then heavy end pieces that get weighed down and cause the whole puzzle to fall off the table. There is some recourse, however, and it can be recommended that focusing on privacy and security education can and will cause a positive shift towards users being more cautious and safe, keeping their security and privacy in mind.

Our results showed, in majority, that while participants were aware of what it takes to be secure, they often opted not to, which is quite significant, as education is a key piece in creating a better environment for security and privacy. Despite this education and clear understanding, they still chose to practice methods of security and privacy that did not increase their levels of security. On the other hand, they did not necessarily do anything to compromise this security, which is in line with our original study, which showed that people did not increase or decrease security when it came to password expiration policies and their effects.

We conclude that our study answers our research questions and meet our expectations of the results, based on the findings of the original study. The negative effects of password expiration policies are not as severe as previously believed, and the positive effects of these policies are actually more present than previously believed as well. That is not to say, however, that there are no negative effects, just that they are not to the level as what is accepted. This of course warrants additional study, as our limited study does not account for all university students in the state, nation, or internationally.

7. What We Learned

Through this study we have learned that there are a wide variety of ways that people manage their passwords. We discovered that users use different tactics that revolve around convenience for their user experience. If a user is required to learn or educate themselves about a better tactic that is more secure, then it is likely that the user will not engage in the security practice because it poses an inconvenience to the user's experience.

Through conducting this study, we learned that in the future it is better and more efficient to present participants with a shorter survey. We found it difficult to have people complete our survey due to its length and we believe that in future studies posing several short surveys over a longer period of time could prove beneficial to gaining more participants.

8. References

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

[2] 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.

[3] 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.

[4] 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.

[5] D. Florˆencio 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

[6] 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.

[7] S. Gaw and E. W. Felten. Password management strategies for online accounts. In Proceedings of the Symposium on U

[8] G. Notoatmodjo and C. Thomborson. Passwords and perceptions. InProceedings of the AustralasianConference on Information Security (ACISP), pages 71–78, 2009.

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

[10] D. Flor^encio and C. Herley. Where do security policies come from? InProceedings of the Symposium onUsable Privacy and Security (SOUPS), pages 10:1–10:14, 2010.

[11] 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. InProceedings of theSymposium on Usable Privacy and Security (SOUPS),page 2, 2010.

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

[13] P. G. Inglesant and M. A. Sasse. The true cost of unusable password policies: Password use in the wild.InProceedings of the SIGCHI Conference on HumanFactors in Computing Systems, pages 383–392, 2010.

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

[15] 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.

[16] Hana Habib, Pardis Emami-Naeini, Summer Devlin†, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. User Behaviors and Attitudes Under Password Expiration Policies (SOUPS), 2018.

APPENDIX

A. Password Survey

* Required

2. How old are you?*

- 18-24
- 25-34
- 35-44
- 44+

3. What is your gender?*

- Female
- Male
- Prefer not to say
- Other:

4. What is your race/ethnicity?*

- American Indian or Native Alaskan
- Asian
- White/Caucasian
- Black or African American
- Hispanic or Latino
- Non-Hispanic
- Prefer not to say
- Other:

5. Which of the following best describes your highest achieved education level?*

- High School Graduate
- Some college, no degree
- Associates degree
- Bachelors degree
- Graduate degree (Masters, Doctorate, etc.)
- Prefer not to say
- Other:

6. Do you have a part time job?*

- Yes
- No

Password expiration policies

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

If you have more than one password at UNCC, respond using the one you consider to be your main password.

7. Thinking back to when you first created your password, which of the following methods did you use it? *

❑ 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
❑ 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
❑ I prefer not to answer
❑ Other:

8. Some organizations require their members 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

9. How often do you think your university should require its members to change their main password?*

- Every week
- Every 30 days
- Every 60 days
- Every 90 days
- Twice a year
- Every year
- Never
- Not sure
- Other:

10. The last time you changed your main 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
- ❏ I don’t change my password
- ❏ Other:

11. How often have you used your strategy to change your main 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:
- 12. Why do you change your password this way? (select all that apply) *
- Check 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:

13. When changing your 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 school?*

- My main password is identical to a password I use for another account
- My main password is similar to a password I use for another account
- My main password is very different from any passwords I use for other accounts
- I only have one password

15. How similar is your main workplace password to a password you use for a non-school account?*

- My main password is identical to a password I use for a nonschool account
- My main school password is similar to a password I use for a nonschool account
- My main password is very different from any passwords I use for non-school accounts

16. Where did you learn about changing your password this way? (select all that apply)*

- ❏ Boss
- ❏ Colleague
- ❏ Family Member
- ❏ Friend
- ❏ Internet
- ❏ IT Department at School
- ❏ Other:

17. When I last changed my main password because it had expired, my new password was:*

- Much weaker
- Weaker
- About the same
- Stronger
- Much Stronger
- I don't know

18. 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

19. I find having to change my password due to my school expiration policy difficult.*

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not Applicable

20. I find having to change my password due to my school expiration policy annoying.*

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not Applicable

21. What do you do to help yourself remember your main password?*

- ❏ I let my web browser store it

❏ I store it in a password manager
❏ I store it in an encrypted file
❏ 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:

22. How many times have you been unable to log into your main 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
- 6-10
- 10+

23. What do you need to do to change or recover your main 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:

24. Who or what reminds you in advance of your password expiring to change your workplace password? (select all that apply)*

❏ IT department
❏ Automated Emails
❏ Software
❏ I don't get reminded
❏ Other:

25. When do you get the first reminder to change your main password before it expires?*

- Less than 1 day in advance
- 1 day
- Less than a week
- 1-2 weeks
- 3-4 weeks
- 1 month
- More than 1 month
- Other:

26. How does the reminder impact your effort in changing your 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:

27. Has your main 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

28. What did you do when your password was leaked?

❏ 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:

Password Perceptions Survey

29. Have you ever held a job or received a degree in computer science or any related technology field?

- Yes
- No

30. Are you either a computer security professional or a student studying computer security? *

- Yes
- No

31. 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)? *

- Not important at all
- Not very important
- Neither important nor unimportant
- Important
- Very important

32. 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? *

- Not important at all
- Not very important
- Neither important nor unimportant

- Important
- Very important

33. To keep your account secure, how important is it to change your password periodically? *

- Not important at all
- Not very important
- Neither important nor unimportant
- Important
- Very important

34. To keep your account secure, how important is it to create a password that you do not already use somewhere else? *

- Not important at all
- Not very important
- Neither important nor unimportant
- Important
- Very important

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)

35. Creating a password you have already used somewhere else (either exactly or with small modifications) *

- 1 (Very Harmful)
- ...
- 5 (Not Harmful)

36. Storing the password in a place where others can access it *

- 1 (Very Harmful)
- ...
- 5 (Not Harmful)

37. Not changing the password periodically *

- 1 (Very Harmful)
- ...
- 5 (Not Harmful)

38. Creating a simple password (e.g., with no symbols or digits) *

- 1 (Very Harmful)
- ...
- 5 (Not Harmful)

For each pair, which do you think contributes more to account security?

39. Using a complex password | Storing your password in a safe place or not storing it at all *

- Left contributes much more
- Left contributes slightly more
- Both are equal
- Right contributes slightly more
- Right contributes much more

40. Using a complex password | Creating a password that you do not already use somewhere else *

- Left contributes much more
- Left contributes slightly more
- Both are equal
- Right contributes slightly more
- Right contributes much more

41. Using a complex password | Changing your password periodically *

- Left contributes much more
- Left contributes slightly more
- Both are equal
- Right contributes slightly more
- Right contributes much more

42. Changing your password periodically | Creating a password that you do not already use somewhere else *

- Left contributes much more
- Left contributes slightly more
- Both are equal
- Right contributes slightly more
- Right contributes much more

43. Storing your password in a safe place or not storing it at all | Changing your password periodically *

- Left contributes much more
- Left contributes slightly more
- Both are equal
- Right contributes slightly more
- Right contributes much more

44. Storing your password in a safe place or not storing it at all | Creating a password that you do not already use somewhere else *

- Left contributes much more
- Left contributes slightly more
- Both are equal
- Right contributes slightly more
- Right contributes much more

45. Suppose your school's expiration policy changed and your main account password will no longer expire. Going forward, how would you remember your main 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:

46. How often do you change the password of your main account? *

- Never
- Every Week
- Every month
- Every few months
- Every year
- Other: