User Perceptions of Five-Word Passwords

Xiaoyuan Wu
The George Washington University
Washington DC, USA
wxyowen@gwu.edu

Collins W. Munyendo
The George Washington University
Washington DC, USA
cmunyendo@gwu.edu

Eddie Cosic
The George Washington University
Washington DC, USA
eddiecosic@gwu.edu

Genevieve A. Flynn
The George Washington University
Washington DC, USA
genevieveflynn@gwu.edu

Olivia Legault
The George Washington University
Washington DC, USA
olegault@gwu.edu

Adam J. Aviv
The George Washington University
Washington DC, USA
aaviv@gwu.edu

ABSTRACT

Human-chosen passwords are often short, selected non-uniformly, and thus, susceptible to automated guessing attacks. To help users to select more secure but memorable passwords, experts have recommended the use of passphrases of multiple words or phrases. In this paper, we explore a strategy for passphrase selection, so-called *five-word passwords*, where users are assigned five random words for a passphrase. Such a password composition policy was recently adopted at Georgetown University in December 2020. Through a two-part online survey (n = 150 and n = 116), participants selected a five-word password under different conditions. We find that computer-generated five-word passwords are more diverse and likely more secure than five-word passwords users select themselves. While all cases of five-word passwords are likely more secure than a human-generated, traditional password, participants expressed misconceptions regarding the security of five-word passwords (and passwords generally). Five-word passwords also appear to negatively impact usability, only 39.7 % of participants successfully recalled their password after two weeks. While five-word passwords offer improvements for security, more outreach is needed to explain their security benefits and reduce usability burdens.

CCS CONCEPTS

• **Security and Privacy → Authentication**.

KEYWORDS

Security, Passwords, Passphrases, Five-Word Passwords

ACM Reference Format:
Xiaoyuan Wu, Collins W. Munyendo, Eddie Cosic, Genevieve A. Flynn, Olivia Legault, and Adam J. Aviv. 2022. User Perceptions of Five-Word Passwords. In *Annual Computer Security Applications Conference (ACSAC '22), December 5–9, 2022, Austin, TX, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3564625.3567981

ACSAC '22, December 5–9, 2022, Austin, TX, USA

ACM ISBN 978-1-4503-9759-9/22/12…$15.00
https://doi.org/10.1145/3564625.3567981

1 INTRODUCTION

Passwords are the most widely-used mechanism to protect online user accounts [6, 7, 23], in spite of previous studies indicating that most users choose short [22] and weak passwords that can easily be guessed [5, 16, 36]. Many users also frequently reuse passwords across different accounts [13] due to either the large number of accounts they have to manage [16, 22, 53] or perceived inconvenience [46]. Consequently, if one of these accounts is compromised, all other accounts protected by that password are vulnerable [28].

Several suggestions have been advanced to improve password security, including password rotation [10, 65], password composition policies [26], password strength meters [56], and password managers [27]. However, password composition policies have been shown to lead to unusable passwords [26], and password rotation policies have proven detrimental to security [10, 65]. If not appropriately designed [56], password meters have been shown to be unusable, especially if they are very strict [58]. Password managers, while promising, are still plagued by usability challenges [24, 39, 52] that have inhibited their widespread adoption, and password manager users still often select weak passwords [29, 40], only using the password manager to store them [32].

To encourage users to select longer and, thus, more secure passwords, security experts have also recommend passphrases, whereby users select multiple words or phrases as their password [18]. The increased length allows for a greater number of possibilities overall and, thus, makes these passwords quite difficult to guess in an automated way. Starting from December 2020, Georgetown University adopted this policy, requiring all students, faculty and staff to select passwords comprised of five words, so-called *five-word passwords*, to improve security of the university accounts. In this paper, we are interested in exploring the security and usability perception of five-word passwords, asking the following 3 research questions:

RQ1: How usable are five-word passwords?

RQ2: How does the password generation mechanism affect the security and usability of five-word passwords?

RQ3: What are user perceptions of the usability and security of five-word passwords?

To answer these research questions, we conducted a two-part, online survey administered on Prolific [43]. In part 1 (n = 150), participants were asked to generate and recall a five-word password in one of three different ways: (i) Five distinct words were randomly selected from our dictionary and participants could change the five words simultaneously by pressing a button; (ii) Five distinct words

were randomly selected from our dictionary and participants had five buttons allowing them to change any of the words; (iii) Participants chose each of the five words themselves, but each word had to be unique and part of our dictionary. Thereafter, participants were asked about their general password habits, as well as their security and usability perception of five-word passwords, including their likelihood of using these passwords.

Two weeks after part 1, participants were invited back to complete a follow-up, part 2 survey ($n = 116$) that gave them five attempts to recall their five-word password from part 1. If they did recall their password, participants were asked about the techniques they had used to recall their password. We then asked participants to indicate any accounts they had either used their five-word password or would be willing to use outside the study. Lastly, participants were asked about their confidence in the security and memorability of their five-word passwords, as well as any potential improvements that can be made to five-word passwords, generally.

Overall, we find that five-word passwords selected by participants are very secure, with the dictionary size of 1,630 common English words used in generating the five-word passwords leading to a total of 11,435,921,971,539,120 (approx. 2^{53}) possible unique five-word passwords. This makes these passwords quite difficult to guess in automated ways, even with knowledge of the dictionary. However, computer-generated five-word passwords are more random, by definition, compared to five-word passwords selected when participants were free to choose each of the words themselves or the entire phrase. Even then, those five-word passwords are still likely much more secure than user-generated passwords.

While five-word passwords appear to have limited negative impact on short-term recall, they have poor long-term recall rates. Only 39.7 % of participants across treatments were able to successfully recall their five-word password after two weeks. Most participants that did recall their five-word password used tools, such as password managers (PMs), to store their passwords. To improve their usability, five-word passwords can potentially be used alongside password managers, with users generating five-word passwords and then storing them in the PM. This would further address some of the usability challenges that still plague PMs, including the persistence of weak passwords among PM users [40]. Further, users would be able to more easily type five-word passwords on devices where the PM is not installed, compared to the random passwords generated by most PMs by default. 1Password currently has such a passphrase-generation feature [11].

Additionally, participants expressed misconceptions about what makes a password secure. Several participants indicate that five-word passwords are not necessarily secure since they do not have any upper-case letters or special characters. While these additional character-classes can certainly enhance security, their inclusion as part of human-generated passwords does not necessarily improve security [59]. Five-word passwords, on the other hand, are still relatively secure and hard to guess because they are drawn randomly from a large dictionary of words. We argue that it is important for these misconceptions to be addressed if users are to be guided towards selecting stronger passwords, including potentially using five-word passphrases as their password.

2 BACKGROUND

Previous studies have shown that most users have a tendency to choose short and weak passwords, frequently reuse them, and often forget them [16]. Most users express concern over their password security, yet simultaneously perceive the stringent requirements of most security policies as too inflexible, which ultimately impacts their productivity [26]. In response to this, passphrases have been recommended to users [64] to help them select passwords that are longer, and therefore harder to guess, but still memorable.

Five-word passwords are a special case of passphrases where users select five unique words to form a password, with each of the words separated by a dot e.g. *this.could.bee.your.password*. Five words randomly drawn from a sufficiently large dictionary can be easy to remember but extremely difficult to guess, especially in the case of an online attack [18]. In this study, we explore the security and usability impact of five-word passwords generated in three distinct ways: (i) *Treatment 1* – five distinct words are randomly selected from our dictionary and users can change the five words simultaneously by pressing a button; (ii) *Treatment 2* – five distinct words are randomly selected from our dictionary and participants have five buttons allowing them to change any of the five words; (iii) *Treatment 3* – participants create each of the five words, but each word must be unique, comprised of at least three characters and part of our dictionary. Figures 1, 2 and 3 show how five-word passwords were generated across these treatments.

Our dictionary comprised 1,630 distinct English words, with the minimum length of every word restricted to three characters and the maximum restricted to six characters. To create our dictionary, we first identified the 3,000 most common words in English [15]. After removing either short or long words as well as vulgar words, we ended up with a total of 1,630 unique words. We analyze the security of selected five-word passwords by exploring the diversity of selected words, uniqueness of words as well as length of words selected as part of the passwords. We additionally report participants' perception of both security and usability of five-word passwords, as well as their password management habits and behavior, generally.

3 METHODOLOGY

In this section, we describe the two parts of the survey and the treatments used for selecting passwords. Following, we detail the recruitment process, ethics and limitations of our study.

3.1 Survey Part 1: Initial Survey

In the initial survey ($n = 150$), participants were asked to create, confirm and recall a five-word password. They were further asked about their password management habits, generally, which informs if they would likely use a five-word password.

(1) *Informed Consent*: Participants were first informed about the purpose of the study, expected duration and potential benefits in participating. They had to consent to proceed.
(2) *Overview*: Participants were given an overview of the survey procedure as well as an explanation of five-word passwords. They were also informed about the follow-up survey.
(3) *Context for Password Generation*: Participants were asked to imagine a scenario requiring them to generate a new password,

Table 1: Treatment distribution in both parts of the survey.

	Treatment 1		Treatment 2		Treatment 3		Total
	No.	%	No.	%	No.	%	
Part 1	50	33.33	50	33.33	50	33.33	150
Part 2	38	32.76	38	32.76	40	34.48	116

specifically a five-word password. The wording varied depending on the treatment; more details are available in Section 3.3.

(4) *Five-Word Password Creation*: Based on the treatment, participants were asked to create and confirm a five-word password, and then recall it. If the participant failed to recall their password in five attempts, they were asked to generate a new one.
(5) *Password Habits*: Participants were asked about their password habits, including the approximate number of passwords they use and the techniques used to create them (**S1**–**S5**).
(6) *Mid-Survey Recall*: Participants were asked to recall their five-word password and if they could not after five attempts, they regenerated a new five-word password in the same treatment.
(7) *Reflection*: Participants were asked the reason for selecting their five-word password, circumstances they would use it and likelihood of remembering this password (**S6**–**S14**).
(8) *Demographics*: Participants were asked about their demographic information, including gender, age and technical background. We asked these questions last to prevent them from interfering with the rest of the study following Redmiles et al. [45].
(9) *Post-Survey Recall*: Participants were asked to recall their five-word password for a third and final time.

3.2 Survey Part 2: Followup Survey

Participants that completed part 1 were invited back for the follow-up part 2 ($n = 116$) after two weeks. They were asked to recall their password as well as provide their general perception of security and usability of five-word passwords.

(1) *Informed Consent*: Participants were first informed about the purpose and duration of the survey as well as potential benefits in participating. They had to consent once more to proceed.
(2) *Five-Word Password Recall*: Participants were asked to recall the five-word password they created in the first survey and if they could not after five attempts, their five-word password was displayed to them before they proceeded with the survey.
(3) *Five-Word Password Questions*: Participants were asked about the methods they used to recall their five-word password and situations in which they would use or were already using this password outside the study (**Q1**–**Q6**).
(4) *General Five-Word Password Questions*: Participants were asked about their security perception of five-word passwords, and how these passwords can be improved (**Q7**–**Q11**).

3.3 Treatments

In creating their five-word password, each participant was randomly assigned to one of three treatments, treatment 1, treatment 2 or treatment 3 (see Table 1), each with a different mechanism for generating a five-word password (see Figures 1, 2 and 3). We used a dictionary of 1,630 distinct words in generating these passwords.

Table 2: Participants' demographics in both surveys.

		Part 1	Part 2
Gender	Female	74	61
	Male	70	50
	Non-binary	6	5
Age	18 - 24	38	31
	25 - 34	66	51
	35 - 44	22	16
	45 - 54	19	15
	55 - 64	4	3
	Prefer not to say	1	0
Education	High School or equiv.	18	16
	College or Trade	39	35
	Associate's degree	8	7
	Bachelor's degree	45	32
	Master's degree	33	22
	Doctorate	6	4
	Prefer not to say	1	0
Background	Technical	46	30
	Non-Technical	98	82
	Prefer not to say	6	4

(1) *Treatment 1 (Part 1: $n = 50$, Part 2: $n = 38$)*: Five distinct words were randomly selected from our dictionary and connected by four dots in-between to form a five-word password. Participants could press a button to change all five words simultaneously for a new password. Further, they were able to generate a new five-word password until they were satisfied with their choice.
(2) *Treatment 2 (Part 1: $n = 50$, Part 2: $n = 38$)*: Five distinct words were randomly selected from our dictionary and connected by four dots in-between to form a five-word password, similar to treatment 1. However, participants had five buttons to change each word individually as many times as they preferred.
(3) *Treatment 3 (Part 1: $n = 50$, Part 2: $n = 40$)*: Unlike treatment 1 and 2 that generated passwords, participants in this treatment created their own five-word password subject to the following constraints: (i) Each of the five words had to comprise of at least three characters and be in our dictionary. (ii) The password had to comprise of five words with a dot between each of the words. (iii) None of the five words could be repeated.

3.4 Recruitment

We recruited participants through Prolific, an online survey distribution platform. The first part had $n = 150$ participants, of which all were invited back two weeks later for the second, followup survey, of which $n = 116$ completed. In both parts, more than half of the participants were female, primarily younger and more well-educated than the general United States population. Participants were compensated $2.50 for part 1, completing it on average within ten minutes, and $1.00 for part 2, completing it on average within five minutes. All participants were required to reside in the United States using Prolific's qualifications settings. Table 2 contains the full demographic information of participants in both parts.

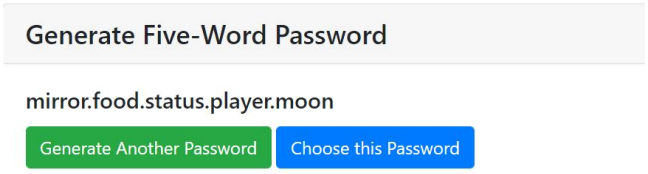

Figure 1: Treatment 1.

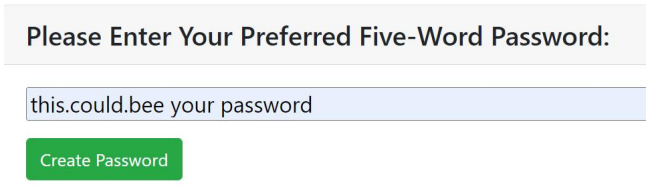

Figure 2: Treatment 3.

Figure 3: Treatment 2.

3.5 Qualitative Data Analysis

Questions **S2**, **S4**, **S5**, **S6**, **S7**, **S8**, **S11**, **S12** from survey 1 and **Q5**, **Q6**, **Q8**, **Q10**, **Q11** from the second survey are open response questions and as such, were analyzed qualitatively. To create a descriptive theme for each question, one researcher created a primary codebook that encodes responses from all the participants. A second researcher then used this codebook to code 30% of the responses before inter-coder reliability was calculated. If high agreement was not reached ($\kappa > 0.7$), the two researchers met to collaboratively resolve discrepancies until agreement was reached. On average, it took 1.5 rounds of coding for agreement across all the questions.

3.6 Limitations

There are a number of limitations with the study. As is typical with online surveys, it is not possible to determine if participants followed all the instructions provided, but we mitigated this by reviewing open-responses for consistency and fullness of text. We did not identify any responses that were inconsistent. The recall rates in part 1 occur after a short time period, less than 10 minutes, but this does model the selection, confirmation, and initial login that would occur with a new password. To better understand recall rates, we use the follow-up survey. Another limitation of this online study is that we do not know why 38 of the 82 participants who used external help were still unable to recall their five-word password in the follow-up survey; we are aware, however, that most participants who recalled their five-word password used external help.

There may also be usability challenges in selecting five-word passwords as we restricted the set of dictionary words. Some participants noted that there were passwords they could not select, notably in the third treatment. A lack of familiarity with the words may also have led some participants to have lower recall rates than might occur in the wild. Additionally, due to the example password we provided – **this.could.bee.your.password** – we observed a preference bias for the use of the word "this", however, such a bias may exist in the wild as describing a five-word password selection procedures would likely require some form of an example.

Lastly, our sample size was relatively small and more educated and may therefore not generalize to the US population as a whole. However, the contexts where five-word passwords are currently required – namely, at Georgetown University – the demographics of the survey may match this cohort well and could generalize.

3.7 Ethical Considerations

This study was approved by our Institutional Review Board (IRB) with approval number `NCR213631`. Participants were fully informed about the potential risks associated with participating at the beginning of both surveys. Some participants also expressed interest in using the five-word passwords they created to protect their accounts. While we collected all five-word passwords generated by participants, no personal identifiable information was collected to minimize risks of any potential disclosures. All passwords were analyzed separately from the Prolific IDs. Furthermore, we do not present any of the five-word passwords selected as some participants indicated they are already using them outside this study.

4 RESULTS

In this section, we first describe participants' general password management habits. Following, we discuss features as well as the security and usability of five-word passwords they selected. Overall, we find that most five-word passwords selected across treatments are diverse enough to make them quite hard to guess, but add significant usability challenges. At the same time, several participants appear to have misconceptions about password security. In the rest of this section, we discuss these results and their implications.

4.1 General Password Habits

Strategies for Creating Passwords. In the initial survey ($n = 150$), we asked participants to imagine they were joining a new company and explain how they would create a password for a new account (**S4**). A majority of participants 62% ($n = 93$) indicated they would use some combination of letters, numbers and symbols. Of these, 36 said they would use all three while 20 reported they would use two

types, either letters and numbers, numbers and symbols or letters and symbols. A further 46 participants said they would use their existing passwords or a slight variation of these passwords, with P121 stating: *"I would most likely keep the same password with a slight change in the numbers or special characters."*

We further asked participants in part 1 (n = 150) to think about the strategy they used when creating their strongest password (**S5**). Most participants (83% n = 125) indicated they used words and symbols when creating their strongest password. Of these, 44 participants used random words and symbols while 36 mentioned personal information including nicknames, important dates or pet names. For example, P198 said:

> *"A word that is special to me, with an important date in the middle, and a symbol at the end. I feel it would be almost impossible for someone else to guess."*

Number of Unique Passwords. Participants were further asked to approximate the number of unique passwords they have (**S1**) in part 1 (n = 150). An overwhelming majority of participants (n = 116, 77.3%) indicated they have 10 or less unique passwords even though prior work has shown that users have about 25 accounts that require passwords [16]. Together with participants' responses to **S1**, it may be the case that these participants likely reuse some subset of their passwords across different accounts.

Password Management. In the initial survey (n = 150), we also asked participants to indicate the strategies they use to manage their passwords across different online accounts (**S2**). Forty-two (28%) participants said they use either the same password or a slight modification of it across accounts, while 39 (26%) participants said they use a password manager. Moreover, 14 (9.33%) participants mentioned they have a set of passwords to use for specific types of accounts. As an example, P162 stated:

> *"I have one password for all my streaming services; one for all my banking/finance; one for personal email; one for work email and work accounts."*

4.2 Features of Five-Word Passwords

In this section, we describe the frequency of words across the three treatments followed by uniqueness and length of words used in the five-word passwords selected by participants.

Frequency of Words. In analyzing the frequency of words in participants' five-word passwords, we only consider the final password selected by each participant. Figure 4 and 5 summarize the frequency distribution of the most common words selected across each treatment. In treatment 1 and 2 where the five-word passwords were computer-generated, the most common words appeared very few times. For treatment 1, the words *escape, letter* and *pair* were the most common, with each word appearing three times in different participants' passwords, while a further 17 words appeared in two passwords. For treatment 2, the word *mood* was the most common, appearing three times. There were a further eight words that appeared two times in this treatment. This suggests that computer-generated five-word passwords can be very random and therefore relatively secure, even when users are allowed to regenerate them.

For treatment 3 where participants were instructed to choose each word in their five-word password, the word *this* appeared 15 times. The high frequency of the word is likely caused by the provided password example – **this.could.bee.your.password** – during password selection. Nonetheless, there were seven different words that appeared over 3 times, the highest of which were the words *love* (9 times), *could* (6 times), the (6 times), *and* (5 times), *water* (5 times), *cat* (4 times) and *your* (4 times). An additional 35 words appeared two or three times. The increased appearance of certain words is likely due to participants' familiarity with those words, confirmed in our qualitative analysis. Despite the word length and distinct word requirements, providing users with the ability to generate their own five-word passwords may still result in weak passwords. The usage of appropriate blocklists where common words are blocked, similarly recommended for Android unlock patterns [37] and PINs [30, 31], could potentially help alleviate this issue. This is a promising area for further research.

Table 3: Length of words in each treatment.

Word Length	Treatment 1	Treatment 2	Treatment 3	Total
Length 3	40	27	59	126
Length 4	86	65	101	252
Length 5	61	83	63	207
Length 6	63	75	27	165
Avg. Length	4.59	4.82	4.23	4.55

Order of Words. We also examined the order of words in participants' five-word passwords. Across all the treatments, the word *this* appeared 14 times as the first word, followed by *the* which appeared three times. Eleven other words appeared twice in the first position. The word *could* was the most popular second word, appearing six times, while *love* and *blue* appeared four and three times respectively. An additional 14 words appeared twice in this position. For the third word, 11 words appeared twice while for the forth word, the words *your* and *and* appeared four and three times respectively. Finally, for the fifth word, the word *six* appeared three times with 10 other words appearing twice.

When analyzing the order of words across individual treatments, we found no particular relationship between words and their position in the five-word password. However, when participants were asked to come up with their own five words in treatment 3, we noted that words that usually begin a sentence (e.g. *this* and *the*) appear frequently in the first position while other words such as *love*, *could* and *your* appeared between positions two and four. While some of these words' increased frequency is likely caused by the example we provided (as previously mentioned), others are likely caused by participants coming up with five words the same way they talk or write in English. Exploring the impact that this has on security and usability is left for future endeavors.

Uniqueness of Words. To understand how diverse the words in participants' five-word passwords are, we looked at how many unique words were present in their passwords. Compared to treatment 3, treatment 1 and 2 had more unique words in selected five-word passwords, with each having 227 and 240 unique words respectively. In contrast, treatment 3 had only 162 unique words. This once again suggests that computer-generated five-word passwords

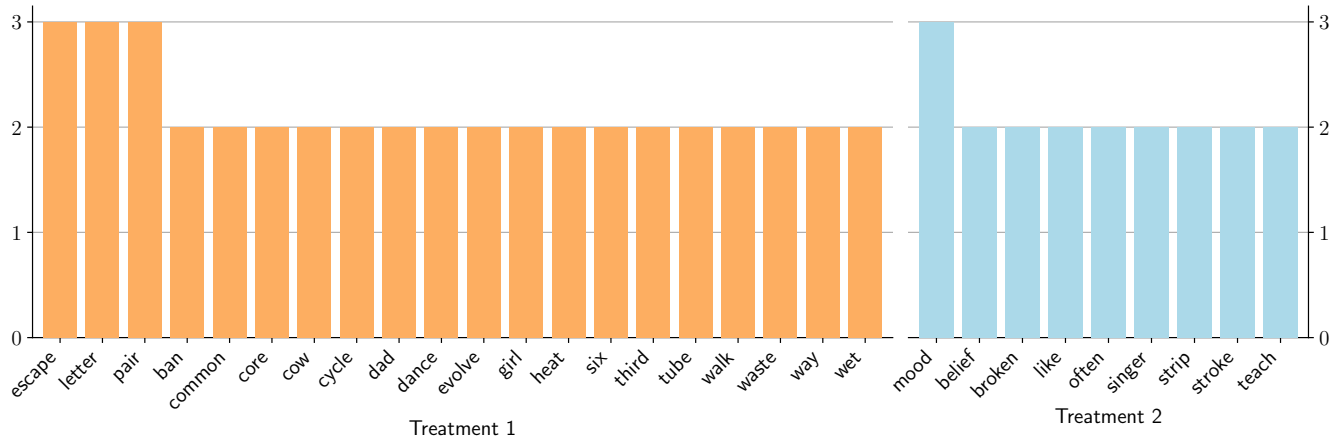

Figure 4: Frequency of words that appeared at least twice in treatment 1 and treatment 2.

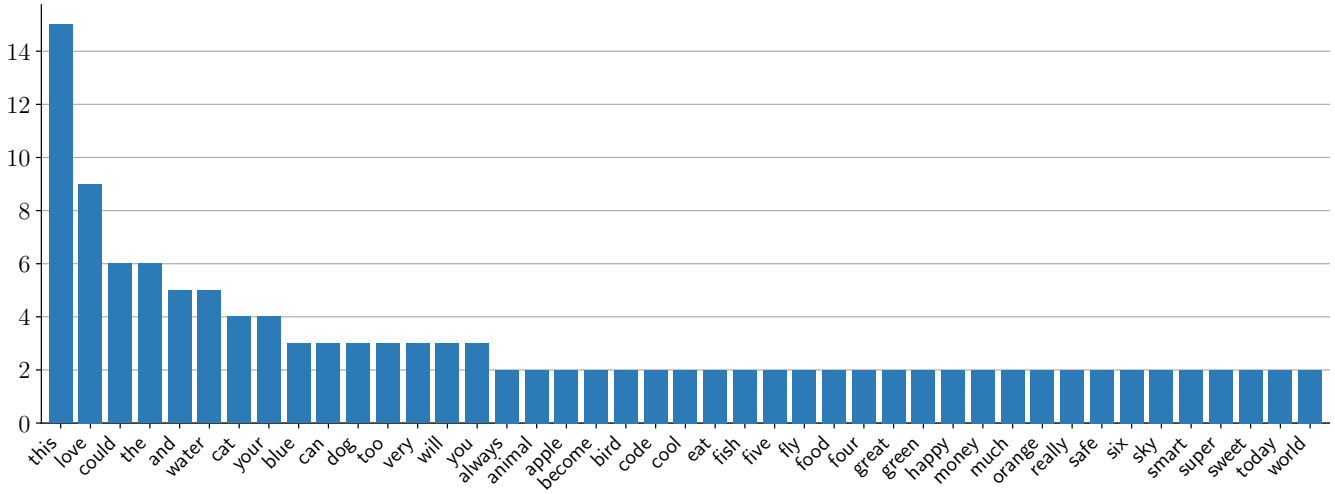

Figure 5: Frequency of words that appeared at least twice in treatment 3.

can be more diverse, and subsequently more secure in comparison to five-word passwords where users select each of the five words.

Length of Words. Table 3 shows the length of individual words selected as part of five-word passwords across the three treatments. With the 1,630 words from our dictionary having an average length of 4.78, we found the average length of the 750 words chosen by participants across the 3 treatments to be 4.55. Words in treatment 3 were relatively shorter (4.23) in comparison to treatment 1 (4.59) and treatment 2 (4.82). When comparing the three treatments, we found that participants in treatment 3 tended to select shorter words.

4.3 Security of Five-Word Passwords

In generating participants' five-word passwords, we used a dictionary comprising of 1,630 unique English words. Even with this modest dictionary size, there exists 11,435,921,971,539,120 (approx. 2^{53}) possible combinations of unique five-word passwords. This makes it very difficult to guess these passwords even with knowledge of the dictionary used. However, participants tended to select common English words when allowed to select each of the five words themselves. Further, some words including *"the"* tended to appear at the beginning of five-word passwords, similar to the English sentence structure. While this implies that attackers can leverage Natural Language Processing techniques to compromise these passwords, the high number of possible combinations still makes this very unlikely. Our study did not simulate such attacks due to the relative sparsity of data; this can be investigated in future.

4.4 Usability and Perception

Five-word Password Creation. To quantitatively measure the effort needed to create a new five-word password, we recorded the number of times participants regenerated their five-word passwords in the case of treatment 1 and 2. This is summarized in Table 4. In treatment 1, participants, on average, regenerated their password

Table 4: Number of times participants (re)generated their five-word password in treatment 1 and 3 or (re)generated each individual word in the case of treatment 2.

	Average	Minimum	Maximum
Treatment 1	10.84	1	87
Treatment 3	1.04	1	2
Treatment 2			
Word 1	4.94	1	57
Word 2	5.18	1	78
Word 3	3.44	1	32
Word 4	4.08	1	41
Word 5	6.84	1	144

10.84 times, with only seven participants choosing the first five-word password that was generated for them. One participant even regenerated their five-word password 87 times. For treatment 2 on the other hand, we recorded the number of times participants regenerated each of the five words. Participants, on average, re-generated each word 5 times (or 25 times for the whole five-word password). In terms of the maximum number of times a word was regenerated, one participant regenerated their fifth word 144 times, ultimately settling on the word *girl*. While treatment 2 gives users more freedom to regenerate each of the five words individually, it also seems to increase the number of times users regenerate the words overall when choosing their five-word password.

To understand reasons why participants settled on their preferred five-word password in part 1 ($n = 150$), we qualitatively asked them for their reason for choosing this password in **S6**, **S7** and **S8**. Eighty percent ($n = 40$) of participants from treatment 1 and 64% ($n = 32$) from treatment 2 indicated settling on their selected five-word password because it was easy to remember, matching inquiries from prior work [8, 37, 38] regarding strategies for password selection. In particular, nine (22.5%) participants from treatment 1 and 12 (37.5%) from treatment 2 said the five-word password they chose made sense to them in ways such as, forming a sentence or having a rhythm. For example, P98 from treatment 1 stated:

> *"All the words were short, four of the five had an 'i' and two of the five had 'ai' in the word. All of these characteristics make the password easier to remember. They also made a somewhat coherent sentence which makes remembering it easier."*

When given the option to change each of the five words in treatment 2, P192 indicated changing each of the five words until they found words all starting with the same letter:

> *"I spontaneously decided to have all of the words start with the same letter, so I clicked through until the appropriate word popped up."*

P100 from treatment 3 on the other hand, indicated creating their five-word password by "stick(ing) to a theme so that I could remember the password."

While, on average, participants had to regenerate words in their five-word passwords more in treatment 2 compared to treatment 1, treatment 2 offers the benefit of five-word passwords that make sense to the user, and may thus be easier to remember.

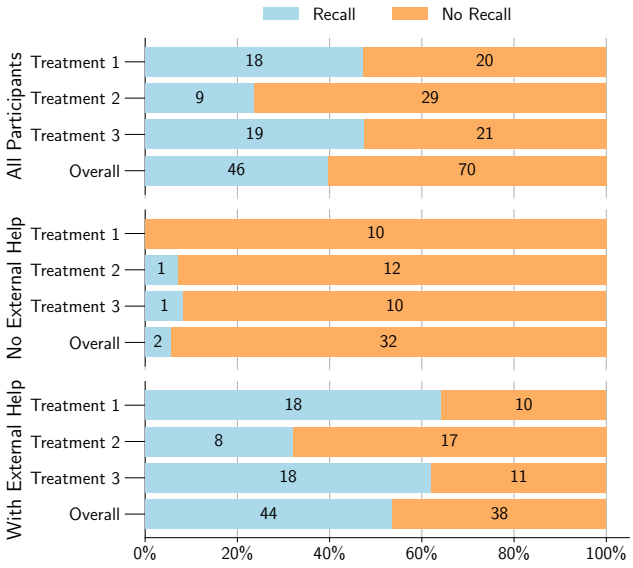

Figure 6: Recall rates after 2 weeks.

Recall Rates. During the course of the initial survey, participants had to recall their five-word password three times: at the beginning of the survey right after generating their five-word password, just before the reflection questions (**S6**, **S7** & **S8**) and lastly at the end of the survey. During the first recall, a majority of participants were able to recall their five-word passwords; all participants in treatment 2 and 98% of participants in treatment 1 and 3 successfully recalled their passwords. There was a slight decrease in recall rate for the second recall phase, with 44 participants (88%) in treatment 1, 48 participants (96%) in treatment 2 and 43 participants (86%) in treatment 3 recalling their passwords. During the final recall at the end of the survey, however, all participants in treatment 1 and 2, and 98% ($n = 49$) in treatment 3 recalled their five-word password.

Two weeks after taking the initial survey, participants were invited back to the follow-up survey and given five attempts to recall their five-word password from the initial survey. Figure 6 summarizes these results. Out of the 116 participants that returned for the follow-up survey, treatments 1 and 3 had roughly similar recall rates; 47% ($n = 18$) of participants in treatment 1 and 48% ($n = 19$) of participants in treatment 3 recalled their passwords. Surprisingly, treatment 2 where participants could regenerate all the words had the lowest recall rate, with only 24% ($n = 9$) of participants able to recall their passwords.

For recall during the follow-up survey, we were also interested in exploring the recall rates for participants that did not use any help such as a physical note, a digital file or a password manager (**Q1**) to recall their password. Out of the 116 participants that returned for the follow-up survey, only 34 indicated they had not used any help. We find that the recall rates for these participants were significantly lower, with none of the 10 participants in treatment 1 recalling their password (see Figure 6). In treatment 2, only 1 out of 13 participants recalled their password; this was similar to treatment 3 where only 1 of 11 recalled their five-word password. In contrast, we found

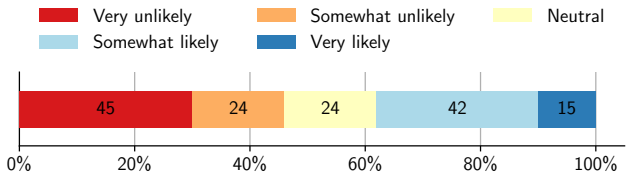

Figure 7: Likelihood of participants using their five-word passwords outside of the study.

over half (54%) of all of the participants who used external help recalled their five-word passwords two weeks later, particularly in treatments 1 and 3 where over 60% of participants successfully recalled their five-word password using external help.

We were also interested in exploring the relationship between the number of times participants regenerated their passwords and recall rates in the follow-up survey. However, we found no correlation.

Overall, we find that five-word passwords have great short-term recall rates, but poor long-term recall rates. While this highlights a potential usability problem, users may be able to recall these passwords if they use them more frequently (cited by nine participants in open responses to question **Q10**). Further, since these passwords are relatively secure, users can potentially be encouraged to employ tools such as password managers to recall them. This would particularly be helpful as users of password managers have been shown not to use the password manager's password generator [32] when creating their passwords, often resulting in weak passwords. Additionally, these passwords would be much easier to type on devices where the password manager is not installed in comparison to the random passwords generated by PMs by default.

Usage of Five-word Passwords. In the initial survey (n = 150), we asked participants about their likelihood of using their five-word passwords outside the study on a Likert-scale (**S14**). Figure 7 summarizes these results. Almost half of the participants (n = 69, 46 %) indicated being very unlikely, or somewhat unlikely to use five-word passwords outside the study. On the other hand, 38 % of participants (n = 57) indicated they were somewhat likely or very likely to use five-word passwords outside the study.

In the follow-up survey (n = 116), we asked participants to indicate all online accounts where they were already using their five-word password outside the study, or would be willing to do. The results are summarized in Figure 8. While several participants (n = 47) indicated they would not consider using five-word passwords on any accounts, a majority indicated they would be willing to use these passwords for either email (n = 40), social media (n = 38), retail websites (n = 35), banking (n = 19) or work accounts (n = 18). Further, five (4%) participants indicated they were already using their five-word passwords on accounts outside the study. Out of these five participants, one indicated using it for their email, three for their social media accounts while one participant indicated using it for both their email and social media accounts. Further, four out of these five participants used external help, for example, a physical note, to remember, and were all able to recall their passwords on their first attempt. One participant did not use any help but was unable to recall their password, despite indicating

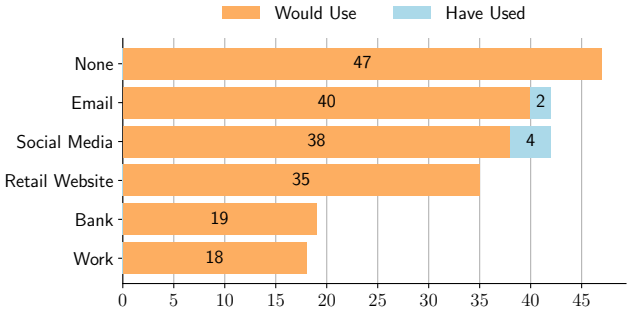

Figure 8: Online accounts where participants used or would use their five-word passwords. Note, participants could indicate multiple accounts.

they were already using this password outside the study. Overall, a majority of participants indicate willingness to use five-word passwords, suggesting that users would likely be receptive of them if they are deployed in the wild.

Security Perceptions. When asked about the security of five-word passwords in the follow-up survey (n = 116) in **Q8**, 83 (71.6 %) participants said they believe five-word passwords are secure while 33 (28.4 %) said they do not believe these passwords are secure. Among the 83 who said five-word passwords are secure, 29 participants indicated they are hard to crack or guess, with P174 stating:

> *"I think people usually make up passwords that don't have the periods or with five words. Hackers would have a harder time coming up with your password."*

P194 similarly added that "computers are good at cracking passwords that are short, five word passwords would have so many characters it would be more difficult to crack with brute force."

A further 10 participants pointed to the length while six participants mentioned randomness as factors that make these passwords secure, with P181 believing five-word passwords are secure:

> *"because of the length of the password. The amount of words and the periods add a decent amount of complexity to the password."*

Regarding randomness, P169 stated that "they could be the most randomest[sic] words that only make sense for the user."

Among the 33 participants who do not believe five-word passwords are secure, 18 participants said it is easy to guess five-word passwords by brute force, with P204 believing five-word passwords are not secure because "password like this without special characters nor numbers is very easy to break with brutal force". A further 12 participants indicated the need to add capital letters, numbers or symbols to make five-word passwords secure, with P136 stating:

> *"i [sic] believe that five words are more difficult to guess and hack into but i [sic] would feel more confident if there were more layers to the complexity of the password, such as numbers and capitalizations."*

Our qualitative results indicate a misconception among several participants about what makes a password secure, similar to prior work [33, 57]. As previously explained, approximately 2^{53} different

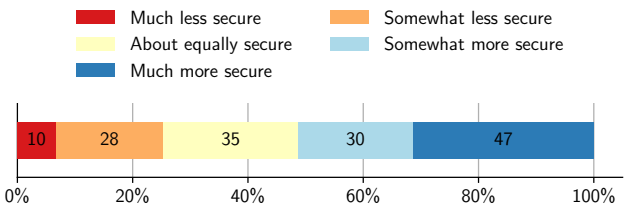

Figure 9: Security perception of five-word passwords versus other passwords.

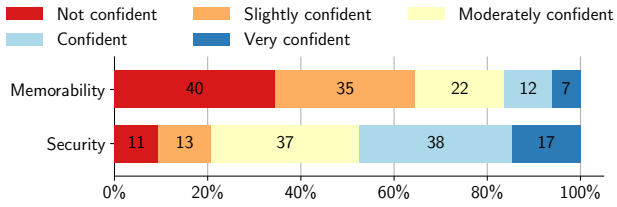

Figure 10: Confidence level in the security and memorability of five-word passwords.

combinations of five words exist from a dictionary of just 1,630 words and therefore, a brute force attack is unlikely to compromise users' five-word passwords, especially for authentication systems that implement throttling. Participants think using words with numbers, capital letters and special characters decrease the likelihood of an attack on their passwords, despite research showing the limited security benefits of this [59] in human-selected passwords. This is likely caused by most websites requiring a combination of lower and upper case letters, numbers as well as special characters during password creation. It is important to address these misconceptions to help users select strong and more secure passwords.

Security of Five-Word Passwords Compared to Other Passwords. In the initial survey (n = 150), we also asked participants to compare the security of their selected five-word password to passwords of other accounts they have. This is summarized in Figure 9. A majority of participants (n = 112, 74.67%) believe their five-word passwords are about equally secure, somewhat more secure or much more secure compared to passwords of other accounts they own. This suggests that most participants would be confident in the security of five-word passwords if they were to be rolled out.

Confidence in Memorability and Security of Five-word Passwords. In the followup survey (n = 116), we additionally asked participants about their confidence level in both memorability as well as security of their five-word passwords. This is summarized in Figure 10. Most participants indicated being slightly confident (n = 35, 30.1 %), moderately confident (n = 22, 19 %), confident (n = 12, 10.3 %) or very confident (n = 7, 6 %) about remembering their five-word password, despite the fact that a majority were unable to recall them. In terms of security, an overwhelming majority believe their five-word passwords are secure, with 91 % (n = 105) participants slightly confident, moderately confident, confident or very confident that their five-word passwords are secure. Only 11 participants (9 %) were not confident that five-word passwords are secure. Overall, participants appear to be confident in both the security and memorability of five-word passwords, despite the poor long-term recall rates.

5 RELATED WORK

Originally intended for controlling access to time-shared mainframe computers in the 1960s [7], passwords have evolved to become the de-facto method of authentication on the web today [6, 7, 23]. This is in spite of previous studies suggesting that many users often select weak passwords that can easily be guessed [5, 16, 22]. For instance, most users prefer short passwords [22] while many others select only lower case letters in their passwords [16] if allowed to do so. Further, due to the numerous accounts that users often have to manage, a majority of users frequently reuse their passwords across different accounts [13, 16, 22, 53, 61]. This unfortunately means that if one account is compromised, then all other accounts using the same password become vulnerable [28].

To improve password security, several recommendations have subsequently been made. One common technique is the usage of password composition policies whereby users' passwords must comply with a set of rules including a set minimum length, usage of special characters and numbers as well as upper and lower case characters. While users are often annoyed by these requirements and struggle to create passwords that comply with them [26], they at the same time believe passwords that comply with these requirements offer better security [51]. In their institution-wide study for instance, Mazurek et al. [34] found that users that expressed annoyance with Carnegie Mellon's password composition policy selected weaker passwords. Nonetheless, other studies have shown that users tend to find workarounds around these policies, with most users specifically adding characters and symbols in predictable places [59, 63] which limits the security benefit of these policies.

Other policies include password expiration policies whereby users are required to change their passwords after a certain period of time to mitigate potential password attacks. However, several studies [10, 21, 65] have shown that these policies offer limited security improvement and may in fact have adverse effects on security as most users choose to slightly modify their passwords. Further, users may actually select weak passwords if they're aware they have to change them in future. Nonetheless, appropriately-designed password policies remain promising [54], particularly if users can get real-time feedback as they create their passwords [50].

To help users understand password creation policies as well as visualize password strength, strength meters have been recently used during password creation. However, prior research has shown that password meters remain constrained by inaccuracies regarding password strength [19, 58]. Ur et al. [58] specifically showed that while strength meters can help users create longer passwords, these passwords are not always necessarily secure. In a followup study, Ur et al. [56] found that data-driven meters that provide detailed feedback to users on their password strength are more effective and can improve password security, similar to the Markov-model based strength meters recommended by Castelluccia et al. [9].

Companies have recently started to monitor and inform their users of potential password reuse for example by comparing credentials posted on the dark web against their users' credentials.

However, research has shown that existing notification systems are not very effective in nudging users to update their reused passwords [20, 25]. Most users tend to ignore these notifications, or only change the passwords of the website they received the notification from, but not other accounts where the password is also reused [20, 25]. In addition, users who do change their leaked passwords tend to make minimal modifications to these passwords, resulting in variations that are likely still vulnerable to attacks [25].

More recently, password managers (PMs) have been widely recommended to users to help them create and recall strong, random and unique passwords across different accounts. However, several studies have found that password managers are still plagued by usability challenges that hinder their widespread adoption and use [24, 39, 52]. Other studies have shown that even users of PMs do not use them effectively, with many still generating weak passwords themselves and only using the password manager to store the passwords [32, 39, 41, 52]. As users struggle to type passwords generated by password managers on devices without the PM, five-word passwords may particularly help fill this gap as they are not only random and secure, but can also be more easily typed on new devices. This is a promising area of future research.

Two-factor authentication (2FA) has also been recommended to further protect users' online accounts. Despite its evident security benefits, adoption of 2FA remains relatively low, with recent reports [44] as well as research studies [42] showing that less than 10 % of Gmail user accounts have enabled 2FA, despite Google rolling out two-factor authentication several years ago. Similar to password managers, however, usability appears to be the biggest factor encouraging or hindering adoption of 2FA [12, 14]. Recent work by Reynolds et al. [47] at two universities found errors to still persist in 2FA systems, inhibiting their adoption. Additional work is required to explore how users can be encouraged to adopt 2FA.

When physical keyboards are scaled down to virtual keyboards on small screens, previous studies have found that the usability of passwords further reduces [35], with users more likely to create even weaker passwords on mobile devices [35] compared to passwords selected on physical keyboards. While Melicher et al. [35] recommend making the passwords visible as users type them to improve both security and usability of passwords created on mobile devices, Schaub et al. [49] found that this unfortunately makes these passwords susceptible to attacks such as shoulder surfing, similar to Android unlock patterns [2, 4].

Beyond alphanumeric passwords, other authentication schemes used on smartphones have been the subject of a lot of research. Many user selected PINs [30, 31, 38, 62], Android unlock patterns [1, 17, 37, 55] and knock codes [48] are chosen non-uniformly, similar to alphanumeric passwords, making a meaningful fraction of them susceptible to guessing attacks. Graphical passwords such as Android unlock patterns are particularly vulnerable to shoulder surfing [2, 4, 60] as well as attacks that use residue and smudges on the screen to reconstruct the pattern [3]. While blocklists have proved effective in making users select more diversely for both PINs [30, 31] and patterns [37], they need to be appropriately sized; this sometimes makes them less usable. Similar to password expiration policies that require users to frequently update their passwords for arbitrary reasons, however, upgrading PINs from 4 to 6 digits has shown limited security benefits [38]. A similar phenomenon has also been observed for Android patterns where upgrading the grid size from 3x3 to 4x4 only has limited security benefits [1].

6 DISCUSSION AND CONCLUSION

Through a two-part online survey, participants created and recalled five-word passwords, and then provided their perception about the security and usability of these passwords. Overall, we find that five-word passwords seem relatively secure, but unfortunately seem to have negative impact on long-term recall. Participants also seem to have misconceptions about password security, similar to prior research [33, 59]. These are further discussed below.

Security of Five-Word Passwords. Even with the modest dictionary size of 1,630 words used in our study, most five-word passwords selected are diverse enough to make them hard to guess, even with knowledge of the dictionary. Our dictionary size results in 11,435,921,971,539,120 (approx. 2^{53}) possible combinations of unique five-word passwords. This makes five-word passwords ideal for online authentication as most website implement rate-limiting to prevent brute-force attacks. While allowing users to select each of the five words themselves seems to lead to more common words in treatment 3, these passwords are still relatively secure. To reduce the occurrences of common words, blocklists could be employed to prevent users from selecting common words, as similarly recommended for PINs [30, 31] and Android unlock patterns [37]. Further, users could potentially be allowed to use a more diverse set of words, even in other languages, to make attacks even more impractical. These are all promising directions of future research.

Misconceptions about Password Security. Our qualitative responses indicate that a meaningful fraction of participants have misconceptions about password security. Several participants indicated that five-word passwords are not secure because of their lack of multiple character classes and symbols. While these can certainly improve security, previous research has shown that most users put them in predictable places [59], severely inhibiting their security benefits. We argue that it is important to explain to users what makes a password secure in order to improve their password behaviour. In addition to this, users should also be informed about the risks of password reuse and how random, computer-generated passphrases that are unique for each account can mitigate such security risks.

Usability of Passphrases. While most participants were able to recall their five-word passwords during the initial survey, long-term recall was poor, with less than half of participants successfully recalling their password after two weeks. While some participants mentioned they would be able to recall their password if they used it everyday, they also mentioned that it would be difficult to recall several unique five-word passwords for each online account they have. Password managers can help address this gap by storing users' generated five-word passwords. This would in fact help address some of the shortcoming of password managers pointed out in previous work [40] including the tendency of users to select weak passwords, and only use the password manager to store them. Additionally, five-word passwords would be much easier for users to enter on devices where the password manager is not installed compared to passwords generated by most password managers by default. This is another promising area of future research.

ACKNOWLEDGMENTS

We thank Michelle L. Mazurek and Micah Sherr for useful discussions about this topic and members of the GWUSEC lab for their feedback on the survey. We also thank all the anonymous reviewers for their insightful feedback, as well as Lorenzo De Carli for shepherding this paper. This material is based upon work supported by the National Science Foundation under Grant No. 1845300.

ARTIFACTS

To foster future research, we have provided artifacts from this paper that are sufficient to run the survey, and generate Tables 1, 2, 3, 4 and Figures 4, 5, 6, 7, 8, 9 and 10. The survey, data and scripts can be found at https://github.com/gwusec/2022-ACSAC-Five-word-Passwords. Please contact the authors for additional requests.

REFERENCES

[1] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. 2015. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Annual Computer Security Applications Conference (ACSAC '15)*. ACM, Los Angeles, California, USA, 301–310.

[2] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '17)*. ACM, Orlando, Florida, USA, 486–498.

[3] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *USENIX Workshop on Offensive Technologies (WOOT '10)*. USENIX, Washington, District of Columbia, USA, 1–7.

[4] Adam J. Aviv, Flynn Wolf, and Ravi Kuber. 2018. Comparing Video Based Shoulder Surfing with Live Simulation and Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '18)*. ACM, San Juan, Puerto Rico, USA, 453–466.

[5] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *IEEE Symposium on Security and Privacy (SP '12)*. IEEE, San Jose, California, USA, 538–552.

[6] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *IEEE Symposium on Security and Privacy (SP '12)*. IEEE, San Francisco, CA, USA, 553–567. https://doi.org/10.1109/SP.2012.44

[7] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. Passwords and the Evolution of Imperfect Authentication. *Commun. ACM* 58, 7 (jun 2015), 78–87. https://doi.org/10.1145/2699390

[8] Joseph Bonneau, Sören Preibusch, and Ross Anderson. 2012. A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In *Financial Cryptography and Data Security (FC '12)*. Springer, Kralendijk, Bonaire, 25–40.

[9] Claude Castelluccia, Markus Dürmuth, and Daniele Perito. 2012. Adaptive Password-Strength Meters from Markov Models. In *Symposium on Network and Distributed System Security (NDSS '12)*. ISOC, San Diego, California, USA.

[10] Sonia Chiasson and Paul C. Van Oorschot. 2015. Quantifying the Security Advantage of Password Expiration Policies. *Designs, Codes and Cryptography* 77, 2–3 (Dec. 2015), 401–408.

[11] Emily Chioconi. 2022. Tip: Use passphrases when you need a secure but easy-to-type password: 1password. https://blog.1password.com/tip-memorable-password-wifi-tv-apps/

[12] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *ACM Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. ACM, New York, NY, USA, 1–11. https://doi.org/10.1145/3173574.3174030

[13] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security (NDSS '14)*. ISOC, San Diego, California, USA.

[14] Jonathan Dutson, Danny Allen, Dennis Eggett, and Kent Seamons. 2019. "Don't punish all of us": Measuring User Attitudes about Two-Factor Authentication. In *European Workshop on Usable Security (EuroUSEC '19)*. IEEE, New York, New York, USA, 119–128. https://doi.org/10.1109/eurospw.2019.00020

[15] EF. 2020. 3000 most common words in English. https://www.ef.edu/english-resources/english-vocabulary/top-3000-words/, as of October 18, 2022.

[16] Dinei Florencio and Cormac Herley. 2007. A Large-Scale Study of Web Password Habits. In *International Conference on World Wide Web* (Banff, Alberta, Canada) *(WWW '07)*. ACM, New York, NY, USA, 657–666. https://doi.org/10.1145/1242572.1242661

[17] Timothy J. Forman and Adam J. Aviv. 2020. Double Patterns: A Usable Solution to Increase the Security of Android Unlock Patterns. In *Annual Computer Security Applications Conference* (Austin, USA) *(ACSAC '20)*. ACM, New York, NY, USA, 219–233. https://doi.org/10.1145/3427228.3427252

[18] Electronic Frontier Foundation. 2016. EFF Dice-Generated Passphrases. https://www.eff.org/dice, as of October 18, 2022.

[19] Maximilian Golla, Jan Rimkus, Adam J. Aviv, and Markus Dürmuth. 2019. Work in Progress: On the In-Accuracy and Influence of Android Pattern Strength Meters. In *Workshop on Usable Security and Privacy (USEC '19)*. ISOC, San Diego, California, USA.

[20] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. 2018. "What was that site doing with my Facebook password?" Designing Password-Reuse Notification. In *ACM Conference on Computer and Communications Security (CCS '18)*. ACM, Toronto, Canada, 1549–1566.

[21] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2018. User Behaviors and Attitudes Under Password Expiration Policies. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX, Baltimore, Maryland, USA, 13–30.

[22] Ameya Hanamsagar, Simon S. Woo, Chris Kanich, and Jelena Mirkovic. 2018. *Leveraging Semantic Transformation to Investigate Password Habits and Their Causes*. ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3174144

[23] Cormac Herley and Paul Van Oorschot. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy* 10, 1 (2012), 28–36. https://doi.org/10.1109/MSP.2011.150

[24] N. Huaman, S. Amft, M. Oltrogge, Y. Acar, and S. Fahl. 2021. They Would do Better if They Worked Together: The Case of Interaction Problems Between Password Managers and Websites. In *IEEE Symposium on Security and Privacy (SP '21)*. IEEE, Los Alamitos, CA, USA, 1626–1640. https://doi.org/10.1109/SP40001.2021.00094

[25] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. 2017. I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails. In *ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, Colorado, USA, 387–391.

[26] Philip G. Inglesant and Angela M. Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *ACM Conference on Human Factors in Computing Systems (CHI '10)*. ACM, Atlanta, Georgia, USA, 383–392.

[27] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No One Can Hack My Min": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX, USA, 327–346.

[28] Blake Ives, Kenneth R Walsh, and Helmut Schneider. 2004. The domino effect of password reuse. *Commun. ACM* 47, 4 (2004), 75 – 78. http://portal.acm.org/ft_gateway.cfm?id=975820&type=pdf&coll=DL&dl=GUIDE&CFID=331330788&CFTOKEN=90066960

[29] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. 2018. Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. In *USENIX Security Symposium (USENIX Security 18)*. USENIX, Baltimore, MD, 203–220. https://www.usenix.org/conference/usenixsecurity18/presentation/lyastani

[30] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2020. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *IEEE Symposium on Security and Privacy (SP '20)*. IEEE, San Francisco, California, USA, 286–303.

[31] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security* 24, 4 (Nov. 2021), 30:1–30:36.

[32] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. 2022. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *USENIX Security Symposium (USENIX Security 22)*. USENIX, Boston, Massachusetts, USA.

[33] Peter Mayer and Melanie Volkamer. 2018. Addressing misconceptions about password security effectively. In *Workshop on Socio-Technical Aspects in Security and Trust (Workshop on Socio-Technical Aspects in Security and Trust)*. ACM, New York, NY, USA, 16 – 27.

[34] Michelle L Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. 2013. Measuring password guessability for an entire university. In *ACM Conference on Computer and Communications Security (CCS '13)*. ACM, New York, New York, USA, 173 – 186. https://doi.org/10.1145/2508859.2516726

[35] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2016. Usability and Security of Text Passwords on Mobile Devices. In *ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, California, USA, 527–539.

[36] Robert Morris and Ken Thompson. 1979. Password Security: A Case History. *Commun. ACM* 22, 11 (nov 1979), 594–597. https://doi.org/10.1145/359168.359172

[37] Collins W. Munyendo, Miles Grant, Philipp Markert, Timothy J. Forman, and Adam J. Aviv. 2021. Using a Blocklist to Improve the Security of User Selection of Android Patterns. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 37–56.

[38] Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv. 2022. "The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits. In *USENIX Security Symposium (USENIX Security 22)*. USENIX, Boston, Massachusetts, USA.

[39] Sean Oesch and Scott Ruoti. 2020. That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX, Virtual Conference, 2165–2182. https://www.usenix.org/conference/usenixsecurity20/presentation/oesch

[40] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. 2022. "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. ACM, New York, NY, USA, Article 33, 23 pages. https://doi.org/10.1145/3491102.3517534

[41] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium On Usable Privacy and Security (SOUPS '19)*. USENIX, Santa Clara, CA, 319–338.

[42] Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-Factor Authentication: Is the World Ready? Quantifying 2FA Adoption. In *Eighth European Workshop on System Security* (Bordeaux, France) *(EuroSEC '15)*. ACM, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/2751323.2751327

[43] Prolific. 2022. Prolific. https://www.prolific.co/, as of June 8, 2022.

[44] Alison DeNisco Rayome. 2018. Google: Less than 10% of Gmail users enable two-factor authentication. https://www.techrepublic.com/article/google-less-than-10-of-gmail-users-enable-two-factor-authentication/

[45] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2017. *A Summary of Survey Methodology Best Practices for Security and Privacy Researchers*. Technical Report CS-TR-5055. UM Computer Science Department.

[46] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *IEEE Symposium on Security and Privacy (SP '16)*. IEEE, San Jose, California, USA, 272–288. https://doi.org/10.1109/SP.2016.24

[47] Joshua Reynolds, Nikita Samarin, Joseph Barnes, Taylor Judd, Joshua Mason, Michael Bailey, and Serge Egelman. 2020. Empirical Measurement of Systemic 2FA Usability. In *USENIX Security Symposium (USENIX Security 20)*. USENIX, Virtual Conference, 127–143. https://www.usenix.org/conference/usenixsecurity20/presentation/reynolds

[48] Raina Samuel, Philipp Markert, Adam J. Aviv, and Iulian Neamtiu. 2020. Knock, Knock. Who's There? On the Security of LG's Knock Codes. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS '20)*. USENIX, Virtual Conference, 37–59.

[49] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, Ulm, Germany, 13:1–13:10.

[50] Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, and Blase Ur. 2015. A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior. In *ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, Seoul, Republic of Korea, 2903–2912.

[51] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, Redmond, Washington, USA, 2:1–2:20.

[52] Frank Stajano, Max Spencer, Graeme Jenkinson, and Quentin Stafford-Fraser. 2015. Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers. In *International Conference on Passwords (PASSWORD)*. Springer International Publishing, Cham, 61 – 73. https://doi.org/10.1007/978-3-319-24192-0_4

[53] Elizabeth Stobert and Robert Biddle. 2018. The Password Life Cycle. *ACM Transactions on Privacy and Security (TOPS)* 21, 3 (2018), 32 pages. https://doi.org/10.1145/3183341

[54] Joshua Tan, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2020. Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-Strength, Minimum-Length, and Blocklist Requirements. In *ACM Conference on Computer and Communications Security (CCS '20)*. ACM, Virtual Conference, 1407–1426.

[55] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *ACM Conference on Computer and Communications Security (CCS '13)*. ACM, Berlin, Germany, 161–172.

[56] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, and William Melicher. 2017. Design and Evaluation of a Data-Driven Password Meter. In *ACM Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 3775–3786. https://doi.org/10.1145/3025453.3026050

[57] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, California, USA, 3748–3760.

[58] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security Symposium (USENIX Security 12)*. USENIX, Bellevue, WA, 65–80. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur

[59] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS '15)*. USENIX, Ottawa, 123–140. https://www.usenix.org/conference/soups2015/proceedings/presentation/ur

[60] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In *ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, Seoul, Republic of Korea, 2339–2342.

[61] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. 2018. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In *ACM Conference on Data and Application Security and Privacy (CODASPY '18)*. ACM, Tempe, Arizona, USA, 196–203.

[62] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. 2017. Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, Abu Dhabi, United Arab Emirates, 372–385.

[63] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In *ACM Conference on Computer and Communications Security (CCS '10)*. ACM, Chicago, Illinois, USA, 162–175.

[64] M. Yildirim and I. Mackie. 2019. Encouraging users to improve password security and memorability. *International Journal of Information Security* 18 (April 2019), 741–759.

[65] Yinqian Zhang, Fabian Monrose, and Michael K Reiter. 2010. The security of modern password expiration: an algorithmic framework and empirical analysis. In *ACM Conference on Computer and Communications Security (CCS '10)*. ACM, New York, NY, USA, 176 – 186. https://doi.org/10.1145/1866307.1866328

APPENDIX

A SURVEY PART 1

Overview

In the following section, you will be asked to generate a five-word password (which will be explained on the next page) and then answer several questions related to this password and your general password management habits. During the survey, you will be asked to re-enter this password several times. If you enter the password incorrectly too many times, you will be prompted to choose a new password.

Five-Word Password Explanation

A five-word password is a password that follows a specific format consisting of 5 separate words connected by the '.' symbol. The following is an example of a potential password:

this.could.bee.your.password

This password will be computer generated, but you will have the ability to regenerate this password as many times as you would like until you reach a password that you prefer. We will ask you to confirm this password is the one you want to use for the study by re-entering it.

Instructions

Treatment 1: Imagine you are going to be assigned a five-word password by your school or employer. Click the button to generate your password. We are going to ask you to memorize this password and enter it at later points in the study. You are allowed to regenerate *this password* as many times as you would like.

Treatment 2: Imagine you are going to be assigned a five-word password by your school or employer. Click the button to generate your password. We are going to ask you to memorize this password and enter it at later points in the study. You are allowed to regenerate *each of the five words* as many times as you would like.

Treatment 3: Imagine you are asked to come up with a five-word password by your school or employer. The individual words within the password must be between length 3 and 8 and will be checked against a dictionary of common words. Please enter your five-word password below with each word separated by a ".", follow the example: *this.could.bee.your.password*

Ask them to confirm this is the password they want to use and then prompt them to re-enter the password to confirm. If it is incorrect after 3 attempts, as them to generate a new password.

Screening Questions

S1 How many unique passwords do you have?
○ I use the same password for every account ○ 2 - 3 ○ 4 - 6 ○ 7 - 10 ○ More than 10

S2 Please describe how your password(s) are managed/used across different online accounts [free text]

S3 Indicate if you use any of the following password management techniques (Select all that apply)
□ I try to remember my passwords without writing them down or storing them digitally.
□ I reset my password every time I log in rather than remembering my password.
□ I keep physical notes of my passwords.
□ I store my passwords as a digital file or files.
□ I save my passwords in the browser (for example, passwords saved in Chrome).
□ I use a third-party password manager (for example, Lastpass or 1Password).
□ I use a system provided password manager (for example, Apple's Keychain).
□ None of the above.
□ Other: please specify [free text].

S4 Imagine you just joined a company or organization and are required by the IT department to create an account, how would you create a password for this account? [free text]

S5 Think of the strongest password you have. How did you create this password? [free text]

Initial Password Recall

Ask participant to provide their five-word password; If they cannot recall in 5 attempts, prompt them to choose a new password based on treatment.

Reflection Questions

S6 *Treatment 1*: Briefly describe your reasons for stopping on this password.

S7 *Treatment 2*: Briefly describe your reasons for stopping on each word.

S8 *Treatment 3*: Briefly describe your reasons for choosing the words you decided on.

Additional Questions

S9 Compared to other accounts where you use a password, please indicate how secure you view the generated five-word password.
○ Much less secure ○ Somewhat less secure ○ About equally secure ○ Somewhat more secure ○ Much more secure

S10 What platforms would you be comfortable using this generated five-word password? (Select all that apply)
□ Bank accounts □ Email accounts □ Work accounts □ Retail websites accounts □ Social media accounts □ None of the above □ Other: please specify [free text]

S11 Please describe any methods you used to memorize the generated five-word password [free text]

S12 Why do you think the technique(s) above was effective? [free text]

S13 If you were asked to recall this generated five-word password in one week, how likely would you be to remember it?
○ Very likely ○ Somewhat likely ○ Neutral ○ Somewhat unlikely ○ Very unlikely

S14 How likely would you be to use a five-word password outside of this study?
○ Very likely ○ Somewhat likely ○ Neutral ○ Somewhat unlikely ○ Very unlikely

Demographic Questions

D1 What is your gender?
○ Woman ○ Man ○ Non-binary ○ Prefer not to disclose ○ Prefer to self-describe [free text]

D2 How old are you?
○ 18–24 ○ 25–34 ○ 35–44 ○ 45–54 ○ 55–64 ○ 65 or older ○ Prefer not to say

D3 What is the highest degree or level of school you have completed?
○ No schooling completed ○ Some high school ○ High school ○ Some college ○ Trade, technical, or vocational training ○ Associate's Degree ○ Bachelor's Degree ○ Master's Degree ○ Professional Degree ○ Doctorate ○ Prefer not to disclose ○ Other: Please specify [free text]

D4 Which of the following best describes your educational background or job field?
○ I have an education in, or work in, the field of computer science, computer engineering, or IT.
○ I do not have an education in, nor do I work in, the field of computer science, computer engineering, or IT.
○ Prefer not to say

Final Password Recall

Ask participant to provide their five-word password. If they cannot recall in 5 attempts, prompt them to choose a new password based on treatment.

Survey Conclusion

Thank you for participating in our survey! Do you have any thoughts or suggestions on the survey? [optional and free text]
You might be invited back for a second survey within 2 weeks upon the completion of this survey.

B SURVEY PART 2

In the previous survey, you have generated a five-word password as well as answered questions revolving around your general password habits and about the five-word password you generated. In this survey, you will be typing out the exact same five-word password and answer several questions about five-word passwords in general.

Password Recall

Ask participant to provide their five-word password. If they cannot recall in 5 attempts, their five-word password is displayed on the screen before they are given a second chance to type in the exact same five-word password.

Reflection Questions

Display participant's five-word password for their reference and ask the following questions:

Q1 What method (if any) did you use to help you memorize the five-word password you just entered?
○ I remembered without writing it down or storing it digitally.
○ I wrote it down as a physical note.
○ I stored my five-word password as a digital file.
○ I saved my five-word password in the browser (for example in Chrome).
○ I used a third-party password manager (for example Lastpass or 1Password).
○ I used a system provided password manager (for example Apple's Keychain).
○ None of the above.

Q2 Have you used your five-word password on any platforms outside of this study?
○ Yes ○ No *If participant has used the five word password:*

Q3 On what platforms have you used your five-word password (Select all that apply)?
□ Bank accounts □ Email accounts □ Work accounts □ Retail websites accounts □ Social media accounts □ Other [free text] *If participant does not use the five-word password:*

Q4 On what platforms (if any) would you use your five word password (Select all that apply)?
□ Bank accounts □ Email accounts □ Work accounts □ Retail websites accounts □ Social media accounts □ Other [free text] *If any platforms are selected above:*

Q5 What is your motivation for using your five-word password for the accounts you mentioned? [free text]

Q6 What do you want to change (if any) about your five-word password? [free text]

Additional Questions

A five-word password is a password that follows a specific format consisting of 5 separate words connected by the '.' symbol. The following is an example of a potential password:

this.could.bee.your.password

Q7 How confident are you that five-word passwords are capable of keeping your online accounts safe?
○ Not confident ○ Slightly confident ○ Moderately confident ○ Confident ○ Very confident

Q8 Please elaborate on your choice of how confident you are about five-word passwords [free text]

Q9 Do you feel confident in remembering several different five-word passwords for your online accounts?
○ Not confident ○ Slightly confident ○ Moderately confident ○ Confident ○ Very confident

Q10 Please elaborate on your choice of how confident you are [free text]

Q11 What do you want to change (if any) about five-word passwords? [free text]

C QUALITATIVE CODES

- **secure (131)**
  hard-guess (16), hard-crack (13), length (10), random (6), unique (6), no-personal (5), not-confident (4), not-enough (4), dots (3), uncommon (2), word-choice (2), no-sense (1), infinit-combo (1), special (1), not-remember (1), only-words (1), prefer-password-manager (1)
- **words-and-chars (125)**
  random (44), personal (30), pet-name (6), easy-to-remember (5), sentence (1), movie (1), favorite (1), anime (1), object (1)
- **easy-to-remember (125)**
  words (9), sentence (7), short (7), humor (4), rythmic (4), theme (4), rhythm (3), story (3), strong (2), word-ordering (2), first-letter (2), frequently-use (2), relatable (1), spelling (1), coherent (1), common-words (1), first-combo (1), secure (1), relate-to-words (1), typo (1), one-syllable (1)
- **no-change (109)**
- **combination (93)**

nums-letters-symbols (25), nums-words-symbols (11), words (9), nums-words (8), personal (7), nums-letters (6), letters-symbols (3), words-symbols (2), letters (2), object-inspiration (1), nums-symbols (1)

- **numbers (60)**
  personal (11)
- **add (57)**
  symbols (28), numbers (18), nums (17), capitals (14), caps (8), special-chars (6), characters (2), acronym (1), punctuation (1), words (1), similar-words (1), favorite-movie-char (1)
- **repeat (53)**
  in-head (22), oral (13), visual (4)
- **words (40)**
  personal (13), work (11), favorite-words (4), company-name (4), random (3), usual-pass (1), company-name-+-CEO-name (1), review (1), last-two (1)
- **same (37)**
  variation (18), change-regularly (1), change-monthly (1)
- **hard-to-remember (36)**
- **not-secure (35)**
  easy-crack (10), only-words (9), add-symbols (5), easy-guess (5), add-nums (5), add-caps (2), breach (1), hack (1), better-than-normal (1), short (1), personal (1), hard-crack (1)
- **memory (32)**
- **usual-pass (31)**
- **write-down (24)**
  photo (2), store (1)
- **no-method (24)**
- **n/a (22)**
- **bad-memory (21)**
- **physical-storage (21)**
- **password-manager (39)**
- **variation (18)**
  usual-pass (14), change-quarterly (1), object-inspiration (1), change-monthly (1)
- **change (18)**
  length (7), words (5), entire-pass (2), first-word (1), into-sentence (1), style (1), word-odd (1), structure (1)
- **unique (17)**
- **browser-storage (16)**
- **surroundings (15)**
- **change-words (14)**
  memorable (3), sentence (2), complex (2), personal (2), no-personal (1), monosyllable (1)
- **sentence (13)**
- **passwordbank (12)**
  variation (2)
- **change-length (12)**
  reduce (7), increase (1)
- **must-use-everyday (9)**
- **acronyms (9)**
- **file-storage (9)**
- **make-easy-to-remember (9)**
- **good-memory (9)**
- **object-inspiration (9)**
  work (6), personal (1), favorite (1)
- **secure-for-some (9)**
- **long (8)**
- **remember-few (8)**
- **hard-to-guess (8)**
- **favorite (7)**
  sayings (1)
- **remove (7)**
  periods (5), words (1), all-s (1)
- **within-dictionary (6)**
  short-words (1)
- **imagination (6)**
- **meanings (6)**
- **nums (6)**
  work (3), personal (2), personal-+-work (1)
- **use-only-one (6)**
- **use-pass-manager (6)**
- **things-on-mind (5)**
- **passwordbank-2 (5)**
  categorized (1)
- **story (5)**
- **change-dots (4)**
- **needs-personal-meaning (4)**
- **personal (4)**
- **device (4)**
  mnemonic (3)
- **passwordbank-3 (4)**
- **get-used-to (4)**
- **random (4)**
- **common (4)**
- **formula (4)**
- **make-familiar (3)**
- **passwordbank-5 (3)**
- **order-matters (3)**
- **phrase (3)**
- **use-method (3)**
- **first-combo (3)**
- **different-format (2)**
- **context (2)**
  meaningful (2)
- **do-not-want-use (2)**
- **better-than-other (2)**
  short (1)
- **accident (2)**
- **next-word (2)**
  secure (1)
- **theme (2)**
- **work-related (2)**
- **not-five (2)**
- **randomly (2)**
  story (1)
- **feelings (2)**
- **unsure (2)**
- **seems-right (1)**
- **make-personal (1)**
- **none (1)**
- **larger-dictionary (1)**
- **good-method (1)**
- **starting-words (1)**
- **hard-remember (1)**
- **unused (1)**
- **only-if-easy (1)**
- **passwordbank-4 (1)**
  categorized (1)
- **passwordbank-6 (1)**
- **forgot-last-word (1)**
- **simple-words (1)**
- **funny (1)**
- **group-pairs (1)**
- **familiar (1)**
- **positive (1)**
  use-in-future (1)
- **nice (1)**
- **secure-enough (1)**
- **like-the-flow (1)**
- **simple (1)**
- **increase-dictionary-size (1)**
- **easy-remember (1)**
- **not-complicated (1)**
- **important (1)**
- **reorder (1)**
- **personal-connection (1)**
- **atypical-format (1)**
- **no-more-secure (1)**
  current-pword (1)
- **like-the-combination (1)**
- **unique-combo (1)**
- **needs-theme (1)**