"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab

Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay,
Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{bur, fnoma, jbees, ssegreti, rshay, lbauer, nicolasc, lorrie}@cmu.edu

ABSTRACT

Users often make passwords that are easy for attackers to guess. Prior studies have documented features that lead to easily guessed passwords, but have not probed why users craft weak passwords. To understand the genesis of common password patterns and uncover average users' misconceptions about password strength, we conducted a qualitative interview study. In our lab, 49 participants each created passwords for fictitious banking, email, and news website accounts while thinking aloud. We then interviewed them about their general strategies and inspirations. Most participants had a well-defined process for creating passwords. In some cases, participants consciously made weak passwords. In other cases, however, weak passwords resulted from misconceptions, such as the belief that adding "!" to the end of a password instantly makes it secure or that words that are difficult to spell are more secure than easy-to-spell words. Participants commonly anticipated only very targeted attacks, believing that using a birthday or name is secure if those data are not on Facebook. In contrast, some participants made secure passwords using unpredictable phrases or non-standard capitalization. Based on our data, we identify aspects of password creation ripe for improved guidance or automated intervention.

1. INTRODUCTION

Despite decades of research investigating passwords, many users still make passwords that are easy for attackers to guess [9, 22, 35, 62]. Predictable passwords continue to cause problems, as evidenced by the recent release of celebrities' private photos obtained in part through a password-guessing attack on Apple's iCloud [11, 37]. While most everyone would prefer a world without the burden of remembering a portfolio of passwords [18, 53], passwords are familiar, easy to implement, and do not require that users carry anything. As a result, passwords are unlikely to disappear entirely in the near future [7]. Although expecting users to remember complex and distinct passwords for dozens of accounts is absurd, single-sign-on systems, software password managers, and biometrics [4] promise to reduce this burden. Passwords also remain useful for frequently accessed accounts, as master passwords for password managers, and as an integral part of two-factor authentication.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

Researchers have identified common, predictable choices that result in easy-to-guess passwords [9, 22, 35, 62]. While some users may be making informed cost-benefit analyses and creating weak passwords for low-value accounts, other users may have misconceptions about what makes a good password. Existing security advice [10, 28, 36, 49, 73] and real-time feedback [1, 12, 15, 32, 59, 63] may be insufficient in disabusing users of these misconceptions.

To understand where users fall short in their attempts to create passwords, we conducted the first qualitative laboratory study of the process of password creation. Whereas analyses of large sets of passwords can reveal common patterns, a qualitative study is better suited to discern precisely why these patterns appear because researchers can probe the rationale behind behaviors through context-based follow-up questions. Prior lab studies of passwords have focused on password management [2, 20, 27, 29, 52, 55], how users cope with password-composition requirements [45, 66], novel password systems [19], and the external validity of password studies [16]. In this paper, we report on the first lab study focusing exclusively on how users craft and compose passwords step-by-step.

We conducted in-person lab sessions with 49 participants, each of whom created passwords for a banking website, news website, and email account in a think-aloud, role-playing scenario. We also explored participants' general strategies and inspirations. This enabled us to pinpoint participants' misconceptions and identify strategies that seem both usable and secure against large-scale guessing attacks, such as an offline attack [6, 31, 70].

We found that most participants had a well-defined process for creating passwords. Commonly, participants either had a base word or a systematic human "algorithm" for generating passwords based on the site. While many strategies led to predictable passwords, some participants successfully mixed unrelated words or crafted unique phrases to create more secure passwords. Some participants desired passwords of different security levels across the three websites, yet nearly half did not, indicating that some people may routinely waste effort creating and remembering strong passwords for low-value accounts. Participants struggled to create passwords that matched their desired security levels, sometimes creating strong passwords that they inteded to be weak, and vice versa.

Participants were concerned primarily with targeted attacks on their passwords, rather than large-scale, automated attacks. As a result, some participants believed the (common) name of their pets or birthdays would be strong passwords because they had not posted that information on their Facebook page, not accounting for the types of automated guessing attacks often seen in the wild when sites like LinkedIn [9], eHarmony [57], Gawker [5], or Adobe [43] had their password databases compromised.

We identified numerous other security misconceptions. Most participants knew that dictionary words make bad passwords, yet

others incorrectly expected common keyboard patterns (e.g., "qwerty" or "1qaz2wsx") to be a secure replacement. Some participants had learned that phrases make secure passwords, yet chose obvious phrases (e.g., "ilove*SiteName*"). Commonly, participants believed that adding a digit or symbol to the end of a password would make it secure, whereas such an action is very predictable. Other participants conflated difficulty for users with difficulty for attackers, such as thinking that words that are hard to spell are secure.

In contrast, some participants employed strategies that resulted in strong passwords. These strategies included combining unrelated words or developing unique phrases. Whereas many participants insecurely capitalized the first letter of their password in deference to the rules of grammar, others employed non-standard capitalization to make far stronger passwords. Whereas some participants ill-advisedly used the website name as a core part of their password, others used songs and concepts they associate with the site. These related concepts would be far less obvious to attackers.

Many misconceptions we identified might derive from misinterpretations of well-meaning security advice. For example, some participants seem to have misconstrued the idea that "a strong password should contain letters, digits, and symbols" as the false statement "*any* password that contains letters, digits, and symbols is secure." Similarly, the admonition to avoid dictionary words in passwords does not mention birthdays or keyboard patterns, which some participants incorrectly believed to be secure. Building on our results, we discuss aspects of abstract password guidance and data-driven tools that could help users create better passwords by avoiding the misconceptions we observed in this study.

We next discuss related work in Section 2. Then, we present our methodology in Section 3. We present our findings in Section 4, discuss their implications in Section 5, and conclude in Section 6.

2. RELATED WORK

Password-based authentication remains ubiquitous for online accounts [7]. Even if passwords are replaced with devices that do not rely on human memory [41, 53], the deployment of such systems and subsequent decline of passwords would be gradual. Even recent multi-step authentication systems, such as two-factor authentication systems from Google [26] and Microsoft [40], tend to retain passwords as one part of the approach.

The literature on passwords is vast; below, we briefly discuss the most relevant prior work. However, prior studies of password characteristics focus post-facto on passwords that have already been created, in contrast to our qualitative focus on passwords in the process of being created. Prior studies with a similar qualitative approach have generally examined complementary topics, such as password management and novel password systems.

2.1 Analyses of Password Characteristics

Many password databases have been leaked in recent years [5, 9, 43, 57]. Both the popular press and academics have mined these password corpora to identify common passwords characteristics. For example, popular media reported on the leaked set of RockYou passwords, noting the most common password was "123456" [62]. Researchers found that RockYou passwords commonly included digit sequences, names, and phrases about love [69].

Researchers have also focused on the semantic content of passwords [60, 64]. Historically, researchers have found that some of the most prevalent semantic themes in passwords include names and locations [39], as well as dates and years [65]. Researchers have also noted love, animals, and money as common semantic themes [64]. While two-word Amazon payphrases are not as predictable as general English text, common themes include music, television, and sports [8]. Combining multiple words and substituting characters are also common strategies [30].

Other studies have entailed collecting passwords created under controlled conditions in online studies. For example, our group has used this technique to study password-composition policies [31, 38, 51] and password-strength meters [59]. While controlled experiments can be used to collect some behavioral metrics, our qualitative methods allow us to collect far more explanatory data.

We also aim to understand password characteristics. However, qualitatively observing password creation as it happens, rather than after the fact, lets us not just learn *what* users do, but also *why*.

2.2 Laboratory Studies

Other laboratory studies have focused on complementary aspects of the password ecosystem. These aspects have included password-management practices [2, 20, 27, 29, 52, 55] and how users respond to password-creation requirements [45, 66].

Researchers have studied how users recall multiple passwords. Their participants learned six passwords each, including text passwords and graphical passwords. Participants were asked to authenticate two weeks later [13]. Researchers have also explored automatically increasing password strength. Participants created passwords in the lab, and the system added random characters, which participants could shuffle until arriving at a configuration they liked. The authors found that inserting two random characters increased security, yet adding more characters hurt usability [19].

More recently, researchers interviewed 27 participants about their strategies for password management and usage. Participants had an average of 27 accounts and five passwords. They often made tradeoffs between following password advice and expending too much effort [55]. While our methods resemble those of prior lab studies, we are the first to focus on how users create passwords.

3. METHODOLOGY

To uncover precisely how average users construct passwords, we conducted face-to-face interviews in our lab. Participants created passwords for three different types of accounts we hypothesized would elicit different security levels. Each participant created all three passwords under a single password-composition policy that we randomly assigned from three possibilities. Participants engaged in a think-aloud process while creating each password and answered follow-up questions about their processes, decisions, and general habits related to password creation. The study was approved by the Carnegie Mellon University IRB.

3.1 Recruitment and Logistics

We recruited participants for a study on passwords through ads on our local Craigslist and flyers at public places in and around Carnegie Mellon University's Pittsburgh campus. Each session was designed to last between 45 minutes and one hour. We compensated participants $25 for the session. The study took place in a room in our laboratory with either one or two moderators. Participants used a laptop from our lab for the study. We audio-recorded the interviews and subsequently transcribed them.

3.2 Study Protocol

We began the study with demographics questions. We then asked participants to create passwords for three websites while thinking aloud. Next, we asked participants about their general password-creation approach and strategies. Finally, we had participants recall each of their three passwords. The text below provides more detail about each step, and the appendix contains the full interview script.

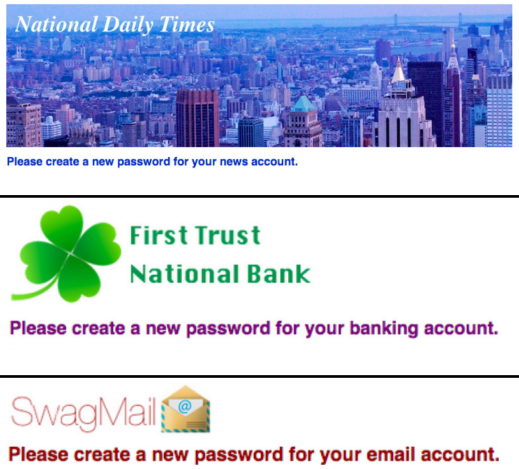

Figure 1: The design of the news (top), banking (middle), and email (bottom) sites for which participants made passwords.

Our demographic questions included age, gender, and occupation. We also asked about familiarity with different computer devices and Internet usage in order to understand the context in which participants created and recalled passwords. In order to introduce participants to the technique of thinking aloud, we next had them perform a warm-up activity in which they thought aloud while crafting a slogan for a bumper sticker.

We then asked participants to create passwords on three different websites, which we assumed would be of different value to participants. These were mock-up websites that we created for the purpose of this study. The three sites, presented in randomized order in the study, were a news website ("National Daily Times"), a banking website ("First Trust National Bank"), and an online email website ("SwagMail"). Figure 1 shows each site's visual design.

We hypothesized that participants would view the password for the news website as having minimal value, whereas the banking and email account passwords would be of higher value. That is, participants would find those accounts more important to protect. Because participants each created three passwords, we could examine the passwords' similarity. Previous research documented that users often reuse passwords verbatim or with minor, predictable modifications [14, 17, 20, 72].

We asked participants to role-play and "pretend that [they] are actually creating new passwords to sign up for new services" and act as if they will "need to use those passwords again to log in to the account [they] sign up for." Furthermore, so that we could understand precisely where in the process of password creation participants came up with different ideas, as well as in what order, we had participants think aloud when creating their password.

Each participant created passwords for all three accounts under a single password-composition policy assigned round-robin from the following three possibilities:

- **1class6**: passwords must include at least 6 characters;
- **2class8**: passwords must include at least 8 characters, among which are at least 2 of the following: a lowercase letter, an uppercase letter, a digit, a symbol;
- **3class12**: passwords must include at least 12 characters, among which are at least 3 of the following: a lowercase letter, an uppercase letter, a digit, a symbol.

As participants met each requirement, a checkmark appeared next to the requirement, as shown in Figure 2. Participants needed

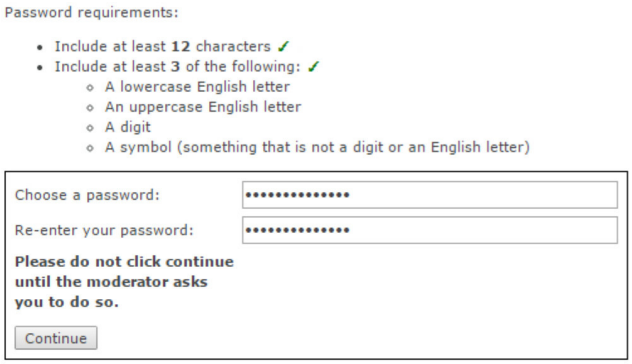

Figure 2: As participants created a password, checkmarks indicated which requirements they had completed. The password appeared as asterisks.

to re-enter their password correctly before proceeding. We chose the 1class6 and 2class8 policies to represent minimal and typical password-composition policies, respectively. We chose 3class12 as a policy that has relatively complex requirements, yet prior research studies have found to be reasonably usable [51]. We expect policies that require longer passwords to see increasing adoption in the real world given the vulnerability of passwords containing eight or fewer characters [24, 54]. We chose to have participants create all three passwords under a single composition policy because we were more interested in how a single participant's behavior differed across sites of potentially different value, as opposed to how a participant's behavior changed across password-composition policies.

We then asked participants about their general strategies for creating passwords and whether the strategies they employed in the study resembled their usual behavior. We excluded from further analysis behaviors they said were atypical. We also asked whether and how they make modifications if they reuse a password, and whether an account of theirs had ever been compromised.

The final part of our study tested password recall. First, to distract participants so that they would think about something other than their passwords for a few minutes, we asked participants to count backward from 100 in increments of seven. Then, we asked participants to log on using each of their three study passwords. We gave each participant up to five attempts to do so, simulating the rate-limiting that many websites use to prevent online attacks.

3.3 Analysis of Password Security

To inform our qualitative analyses of password-creation behaviors, we needed an objective metric of password security. We therefore measured each password's guessability, or how quickly an attacker would guess that password in a large-scale guessing attack [6, 31, 70], using the software tool Hashcat [54]. This tool is widely used by attackers [22, 23, 24, 34, 44] and, relative to other guessing approaches, is generally successful at guessing a large fraction of target password sets in the configuration we used [61]. We made 100 trillion (10^{14}) guesses against participants' passwords, which represents about 6 hours of guessing on a single modern GPU (AMD R9 290x) for passwords stored unsalted using the NTLM hash function, 3 weeks for passwords stored using SHA256, and 904 years for passwords stored using SHA512crypt.

Hashcat takes as input a word list and a set of mangling rules, or transformations (e.g., "add a 1 at the end" or "change every A to @") to apply to word list entries. It is impossible to model every attacker or to study all word lists. We thus chose settings and training data that prior work found to represent a reasonable step

beyond Hashcat's default configuration [61]. Our word list comprised large sets of leaked passwords and natural-language dictionaries. The passwords were taken from breaches of MySpace [48], RockYou [62], and Yahoo! [21]. We used dictionaries found effective in past studies [31, 70]: all single words in the Google Web corpus [25]; the UNIX dictionary; and a 250,000 word inflection dictionary [50]. The combined set of passwords and dictionaries contained 19.4 million unique entries, ordered by descending frequency. The mangling rules comprised the "generated2" set included with oclHashcat and a Hashcat translation of rules originally released by Trustwave SpiderLabs [58] for the tool John the Ripper.

Although this approach simulates a large-scale guessing attack, it does not simulate an attacker who knows personal details of the user. Therefore, members of our research team manually examined the study passwords alongside participants' think-aloud transcriptions. If the password was derived primarily from a date significant to the participant or the name of a participant's family member or pet, we marked the password as vulnerable to a targeted attack. Similarly, if the password was mostly derived from the name of the website on which the participant was making a password, we marked it as vulnerable to an attack targeted to that site. Automated cracking methods do not natively support these sorts of highly targeted attacks, necessitating this limited manual analysis.

3.4 Qualitative Analysis

Because our objective was to gain a nuanced perspective on how users craft passwords, we relied heavily on qualitative methods. Rather than approach the study with well-defined hypotheses or very targeted research questions, we instead chose to let participants' strategies and misconceptions emerge from the data.

To that end, one member of the research team first tagged each self-contained thought, representing a distinct password-creation strategy or behavior, mentioned by any participant either during the think-aloud portion of password creation or in response to an interview question. For example, one of the tagged thoughts was, "swap the g for a $ because gold is something related to money." We identified 546 thoughts across our 49 participants.

The members of the research team then collaboratively analyzed these thoughts in a process derived from affinity diagramming [3]. The members of the research team began with each of the 546 thoughts, as well as the corresponding password, printed out on an individual piece of paper. We then iteratively grouped these thoughts into distinct clusters, continuously refining, collapsing, and separating clusters. These clusters represented thoughts the team felt related closely to each other. At the end of our full-group session, we had grouped these 546 thoughts into 18 initial clusters, with themes such as using the website itself as inspiration for a password or adding random characters to a password.

While these clusters represented closely related behaviors, they conflated secure and insecure actions. To separate successful strategies from security misconceptions, two members of the research team went back through all quotes in each cluster and discussed whether that particular behavior would be beneficial for security, negatively impact security, or whether the security impact was uncertain. As a result, we split some clusters to distinguish between secure variants of a strategy and those that were likely predictable by attackers, transforming the initial 18 clusters into 25 clusters.

Finally, within each of the 25 clusters, we performed an additional round of affinity diagramming to further disambiguate distinct behaviors from each other. For instance, within the broad category of "use words inspired by the website," we created distinct sub-clusters of "passwords derived from the website name," "words a participant associates with the site," "phrases a participant associates with the site," "songs the participant associates with the site," "people the participant associates with the site," "emotions the participant associates with the site," and "descriptions of the website's visual design/logos." This process resulted in 122 distinct behaviors that we report within the context of the 25 broad themes.

In addition to our formative analysis of strategies for creating passwords, we had more targeted research questions related to how participants approach creating and managing passwords. We based these questions on a combination of prior work and our own expectations and experiences. These targeted questions covered the security levels participants desired for different websites, the reuse of whole passwords or elements thereof [14, 72], the order in which participants would think of different chunks of their password [60], and how participants manage passwords [18, 55]. We tagged each instance of a participant discussing or exhibiting behaviors related to these areas. Using the same group process we used to analyze creation strategies, we again clustered these behaviors.

Throughout the paper, we focus on reporting the theme captured by each cluster of behaviors and providing relevant quotes where illustrative. In a few cases, we report the frequency of different behaviors to provide a better sense of our data; these frequencies are not intended to suggest that any quantitative analyses of our data are appropriate. To protect participants, some of whom might have used their real passwords in the study, we adopt Fahl et al.'s suggestion and report in this paper sanitized passwords that replace potentially personalized information with analogous content [16].

3.5 Limitations

Our study suffers from limitations typical of small-scale, qualitative studies. We used a small sample that is not representative of any larger population. For instance, more participants than average have technical backgrounds. Despite these limitations, qualitative studies offer rich insight into not just *what* users do, but *why*. Password characteristics have been very widely studied post-facto, yet the moment-to-moment decisions of password creation had not previously been studied in such depth.

A lab study can only capture a sliver of the many ways in which people use passwords, limiting ecological validity. For example, we had participants create three passwords in succession, whereas password creation for different sites is often spread out over time. Furthermore, we test password recall during the same lab session it was created, albeit following a distraction task. In contrast, users need to recall passwords very frequently for some accounts, yet infrequently for others. Similarly, some users log into accounts using different devices or using password managers, which we do not test. However, only two of the 49 participants reported that they normally use password managers.

Our participants made passwords for a study, not a real account. As a result, they had little incentive to make the passwords hard to guess or easy to remember. To gauge the generalizability of different types of password studies, Fahl et al. compared students' actual university single-sign-on passwords with passwords the same students created for an online or lab study [16]. They found passwords from lab studies to be acceptable proxies for real passwords.

4. RESULTS

Our participants generally wished to create strong passwords, at least for some accounts; they just did not always know how to do so. Even worse, they sometimes wrongly believed their choices were contributing to a strong password even when these choices were actually making the password more predictable. In this section, we discuss the passwords participants actually made, alongside their considerations and micro-decisions along the way.

Table 1: The average length and number of character classes in unique passwords participants created.

Policy	#	Length (characters)			# Classes			
		Median	Mean	σ	1	2	3	4
1class6	37	10	10.1	3.5	6	12	8	11
2class8	47	9	9.9	2.2	–	7	9	31
3class12	47	13	14.4	3.5	–	–	17	30

We begin by describing our 49 participants in Section 4.1. We then briefly summarize the characteristics and guessability of the passwords they created in Section 4.2. Even though many participants made passwords that exceeded the minimum requirements of their assigned password-composition policy, roughly half of the passwords were vulnerable to an automated guesing attack or to a targeted attack. Next, in Section 4.3, we describe participants' desired security level for each of the three sites for which they were creating passwords. Unfortunately, the value participants assigned to accounts diverges from what a security researcher might expect.

The main contributions of this paper rest in the qualitative analyses we detail in the subsequent sections. In Section 4.4, we explore participants' security considerations, as well as their abstract, broad approaches for generating a password. We found that participants try to create passwords to match their perceived value of different accounts. We also found that some participants reused passwords or base elements verbatim across sites. We highlight general approaches and human algorithms participants used to craft a password. Some approaches, such as generating a unique phrase, appear secure and also memorable to participants. Sadly, other participants unwittingly employed very predictable approaches.

Despite their desire to create secure passwords, many participants struggled to distinguish approaches that increase password security from those that make a password easier to guess. In Section 4.5, we delve into participants' low-level strategies and microdecisions. Subtle differences often separated choices that increased security from those that made passwords predictable. For example, basing a password on a song or visual image the participant associates with the website for which he or she is creating a password is far better than using a password like "ilove*SiteName*!" Many of participants' misconceptions can be viewed as twisted interpretations of advice about how to create a strong password.

4.1 Participants

We interviewed 49 participants, 21 male and 28 female. Their ages ranged from 19 to 63. Young participants were overrepresented relative to the general population as the mean age was 31 and the median 24. Of the 49 participants, 24 were students, 13 of whom studied a technical discipline like engineering. Of the non-student participants, 16 were employed in a variety of occupations, while the other 9 were currently unemployed or retired. All participants used text passwords regularly and were frequent Internet users. To preserve anonymity, we refer to each participant as PN.

4.2 Password Characteristics and Security

The 49 participants each created 3 passwords, resulting in a data set of 147 passwords, of which 131 were unique. No participant created the same password as any other participant, but 13 participants reused a password verbatim across two or three of the three accounts. When we report password characteristics and guessability in this subsection, we report on unique passwords, counting a password that a participant reused multiple times only once.

Table 2: The number of passwords created under each policy that were vulnerable to a *general* attack of 10^{14} guesses using Hashcat, as well as the number manually identified as vulnerable to a *site-specific* attack using the website name, or a *user-specific* attack. We also present the number that appear *secure* against all three attacks.

		Vulnerable to attacks			
Policy	#	General	Site-specific	User-specific	Secure
1class6	37	21	0	0	16
2class8	47	19	2	3	23
3class12	47	10	8	3	26

The quantitative metrics we report in this subsection are not intended to suggest generalizability, which would be inappropriate for a small-scale, qualitative study. Instead, we present these numbers to give a broad sense of the passwords our participants created.

Participants often significantly exceeded the requirements specified by their assigned password-composition policy, as shown in Table 1. For example, the median length of a 1class6 password was 10 characters, rather than 6, and 84% of 1class6 passwords included multiple character classes despite the lack of any character-class requirement. Although 2class8 passwords were only required to contain characters from two distinct character classes, 66% of these passwords contained all four character classes.

Across password-composition policies, 38% of the passwords participants created were guessed within 10^{14} guesses in the automated guessing attack using Hashcat. Table 2 gives an overview of how many passwords created under each composition policy were vulnerable to attack. Sanitized examples of passwords vulnerable to this automated guessing are *Tyrone1975* (1class6), *Gandalf*8* (2class8), and *Triptrip1963* (3class12). In contrast, sanitized examples of passwords that were not guessed include *5cupsoftoys* (1class6), *AfNaHiLoco* (2class8), and *7301Poplarblvd$* (3class12). Using lists of common passwords, six passwords were trivially cracked, including three 1class6 passwords (*gabriel*, *password*, and *qwerty*), two 2class8 passwords (*1Qazxsw2* and *Password1!*), and one 3class12 password (*Newspaper123*). None of the other passwords were among the most commonly used passwords [9, 35].

Our automated, large-scale Hashcat attack did not specifically focus on site-specific information, such as the name of the site on which an account was being created. We manually evaluated vulnerability to site-specific attacks, considering a password to be vulnerable if the name (e.g., "First Trust Bank" or "1sttrust") or function of the site (e.g., "email" or "breakingnews") was the majority of the password. We marked ten additional passwords (e.g., *1234SwagMail@* and *nationaldailytimesP@ss2*) as vulnerable.

In addition to general attacks, passwords can also be guessed in attacks targeted to a user's personal information. We manually examined passwords not guessed by Hashcat alongside participants' explanations to determine whether a password would be vulnerable to a user-specific attack. We marked passwords vulnerable if the name of the participant, immediate family member, or pet, or a date or geographic location of well-known significance to the participant, formed the majority of the password. We marked six additional passwords (e.g., structured *Firstname.Lastname715* and *hOMETOWN!123*) as vulnerable.

4.3 Security Level of Each Site

On the assumption that some or all of the participants would create fundamentally different types of passwords based on their de-

sired security for an account, we had participants create passwords for three types of accounts we expected would be of different value: a news site, a banking site, and an email account. We hypothesized that most participants would consider the account on the news site effectively worthless, yet attribute more value to the other accounts.

In stark contrast to our hypothesis, 21 of the 49 participants (43%) considered all three accounts to be of about equal value. Although access to a user's email account can often be used to reset the passwords to his or her other accounts, many participants shared P21's opinion that an "email [account] is not important."

Many of these participants felt the password for the banking account was similarly not much more important than the password for a news site. Although consumer financial protections in the United States would minimize or completely mitigate financial harms of an online banking account compromise, and while additional security features (e.g., security questions) might also help to secure a banking account, few participants explicitly mentioned these factors. P22 was one of the few who did, saying, "Email usually gets the highest security because even if they break into the bank account, the bank often requires you to send something like a special code they sent to your email." Other participants noted that they did not have much money in their bank account and thus did not care about that account. For instance, P48 noted, "As a college student, I don't have a lot of money to worry about." This is despite the fact that identity theft can be ruinous to one's future creditworthiness.

Some of these participants who viewed accounts to be of equal value reused the same passwords verbatim across these sites. Other participants used an identical password-generation technique across these three accounts. P34 was an example of the latter approach, saying he did not "want the same password as with email" for his banking password or the news site. As a result, he cycled through the names of his three brothers, appending "24!" to each to arrive at *Joey24!*, *Johnny24!*, and *Jimmy24!* as his passwords.

Seven participants (14%) felt that their news account was low-value and that their email and banking accounts were of equal (high) value. In some cases, participants reused passwords across accounts they considered to be of the same security level. P44 explained, "I use the same password [as banking] with email because I don't want to remember many passwords." P32 similarly said, "One thing I do a lot is use the same password that are for things about the same security purposes." While such a strategy might be prudent for low-value accounts [18, 42], it may open important accounts to attack. These seven participants felt the news account was worthless. P28, who considered the news site a "junk website," said her approach for "junk websites will be something that's just easy to remember. If it happens to get stolen it won't make that much of a difference."

Another 11 participants (22%) considered the news account and email account low-value, yet felt the banking account was important. As P30 explained, "[Email] is not important to me." Similarly, P41 said, "I don't care about the security of [the news] account," and also said she is "not too concerned about email getting hacked."

The remaining 10 participants (20%) considered all three accounts to be of different value. All thought the news site was lowest value. Eight of the 10 participants considered their banking account more valuable than their email account, while the other two felt their email account was more valuable. P3 said he used "an easier password" for the news account because it "does not have financial" implications, but wanted email "to be a little bit secure."

Many of these participants felt strong pressure to create a secure password. For example, P23 wanted her banking password "to be very secure because if there's any security risk then I would be losing a great deal of money." Similarly, P18 explained, "[Creating a banking password] stresses me out, banking more than even [health] lab results, because I think it's a combination of the fear of identity theft, and draining an account, and relaxing too much, and constantly watching it. I know I want a really strong password. Thinking through how I want to create that is tough."

Sadly, many participants struggled to craft passwords whose actual guessability matched their desired security level. For example, P6 was one of the ten participants who assigned different values to all three accounts. Unfortunately, the only one of her three passwords that was not guessed was her password for the news account, which she intended to be the *least* secure password. Her password for the news account combined dictionary words from two languages with unpredictable capitalization, yet she expected the password to be predictable because it contained dictionary words. In an attempt to craft more secure passwords for the other two accounts, she used permutations of her name and her birthday. Both of these passwords that were intended to be secure were guessed.

Overall, 57% of participants did differentiate across accounts regarding the desired security of their password. Unfortunately, as we detail in the subsequent sections, many of the behaviors these participants thought improved security dramatically had at most a modest impact. The remaining 43% of participants did not differentiate across accounts, potentially resulting in them inefficiently expending their finite memory for passwords [18] on passwords for low-value accounts and thus limiting their ability to remember strong passwords when password strength actually matters.

4.4 General Approach to Password Creation

Of the 49 participants, 43 (88%) said they had a well-defined process for creating passwords that they put into action during the study. In this section, we delve into the approaches we observed.

While password reuse has been studied previously [14, 55], understanding how our participants reused passwords provides essential context. First, we discuss the 13 participants whose general strategy centered on verbatim reuse of a single password. We then discuss the 10 participants who had a base keyword that they reused across sites, making small modifications per password. We also outline other participants' general algorithms for crafting a password, including the order in which they chose different elements to combine into a password. Finally, we briefly mention how password-management strategies [55], impacted participants' expectations and approaches.

4.4.1 Password Reuse

Password reuse is a major threat to password security because the compromise of one account can lead to the subsequent compromise of other accounts for which the user has chosen the same username and password [14]. We found that even when participants expressed a desire to behave securely, they still reused passwords. Only three participants said that, in the abstract, they would never reuse passwords. The other 46 participants said they generally reused passwords. While reusing the same throwaway password for low-value accounts can be an efficient coping strategy, reuse across high-value accounts is risky [18, 42].

In our study, three participants (6%) created a single password and reused it across all three sites because they worried about their ability to remember multiple distinct passwords. Notably, P26, one of the three participants to reuse a single password for all three accounts, had said, "For online banking and things, I try to make my passwords a little more secure," yet reused a password consisting of an obvious keyboard pattern ("1Qazxsw2") for all three sites.

Ten other participants (20%) created only two distinct passwords across the three accounts. Three of these participants had the same

password for the email account and banking site, six participants shared a password for the news site and email account, and one participant used the same password for the news site and banking site. These participants usually failed to see this behavior as potentially problematic. For instance, P2 said he saw "no security downside" in using the same password for the news and email accounts.

Some participants knew in the abstract that password reuse is a poor idea, yet did so anyway. Often, participants found remembering distinct passwords to be too difficult. For example, P6 said it is "very difficult to remember all different passwords." Therefore, she has five distinct passwords that she reuses. P19 reused passwords for accounts she does not think are "that important" and "anything that does not have anything to do with my credit card."

Other participants noted that they had never experienced problems due to password reuse. P1 explained, "I know [password reuse] is a terrible idea, but it does not keep me awake at night....I have never seen any negative consequences." Similarly, P9 said she "usually uses the same password for many things," but is not concerned "because [she has] been using the same password for a long time" and had yet to experience a problem. P45 felt he "should be" worried about consequences of password reuse, yet does not worry.

A number of participants said they did not feel password reuse was a problem because the password they reuse is strong. P2 said he reuses passwords "all the time...if the password is a good one." P35 said similarly, "My [reused] password is not easily guessed," while P49 explained, "No one can guess my [reused] password." Unfortunately, if any site on which that password is reused is compromised and the system administrators do not follow industry best practices (i.e., passwords are salted and hashed using a slow hash funtion like bcrypt [46]), these participants may have multiple accounts compromised if the attacker guesses the password in an offline attack. Notably, during the study, two of these three quoted participants made passwords that they believed were strong, yet were guessed in the general attack using Hashcat.

4.4.2 Element Reuse

Although they did not reuse passwords wholesale, ten participants usually had a long substring in common across their passwords, while eight additional participants sometimes used a common string across passwords. While reusing a base element can still result in strong passwords if modifications and additions to the shared elements are non-trivial, predictable modifications to a base element are common [14, 72]. In those cases, if a single password is compromised, the rest will follow quickly.

In an example of element reuse, P27 used the street name from a former address as his starting point. His email, news, and banking passwords in the study were thus *cedarville1*, *cedarville2*, and *cedarville3a*, respectively. He explained, "I would just go one number up....That way, if I'm having a problem remembering [a password], at least I'll have a base and figure it out from there." He said he would just try increasing digits until landing on the correct password. Notably, he desired for his banking password to be more secure than the others, yet did not achieve this goal. He said, "For a bank, for a little more security, I click it up one number...and add something like another letter." His belief that adding a single "a" on the end makes the password more secure seems misguided. Unfortunately, Hashcat rules to append single characters onto the end of the password are common in lists of mangling rules [34, 54, 58].

P10 also began with a common substring, a mnemonic. His passwords were thus *ATdim12nd#*, *ATdim12sw#*, and *ATdim12ft#*. The two letters that varied represented the names of the sites (*N*ational *D*aily Times, *Sw*agmail, and *F*irst *T*rust). P15 adopted a similar strategy, using "1234" as his starting point and appending a variant of the site name. His passwords were *1234Nat'lDailyTimes*, *1234SwagMail@*, and *1234FirstTrustNat'lBank*.

A common misconception was that making minor or incremental additions to common substrings would result in secure passwords. For example, P37 said she did not care about security for the news site or email account. Therefore, she used *Tyrone* and *gabriel* as those passwords, respectively, drawing on names of family members. However, "because security is required for a bank account," she added Tyrone's birth year, resulting in *Tyrone1975* for the banking site. Unfortunately, the common technique of appending a recent year to a password does not make it secure against a trawling, large-scale attack, let alone against an attacker who researches the user's family members. Similarly, P44 uses the same 8-letter base word across all of his passwords (both in the study and in daily life). For the news account he deemed unimportant, he appended "123." Instead, for the two accounts he wanted to be secure, he appended "1974," his birth year, falling into the same trap as P37. Lists of mangling rules used by attackers frequently include rules that append years to entries in the word list [34, 54, 58].

Other participants expected that character substitutions would similarly transform their typical base password into something more secure. For example, P45 took his shared news and email password, *ninjakick44ninjakick!*, removed the repetition, and instead performed character substitions to arrive at *n1nj@k1ck!* as his banking password. He explained, "I want my banking password to be extra secure... I replaced letters with symbols and numbers to make it secure." Unfortunately, such substitutions are very predictable [60] and provide uncertain security benefit [67].

Similarly, P49 turned her shared news and email password *Elephant0215!*, which she expected to be weak, into the banking password *@El3phant4225*, which she expected to be strong. In particular, she performed a predictable character subsitution, yet also replaced her birthday (02/15), which she expected to be "linked to my bank account," with her favorite four-digit sequence. She also changed the ending exclamation point into a leading "@" because it reminds her of Twitter. While neither password was guessed by Hashcat and both are thus at least moderately secure, these types of modifications would not in general reliably transform an otherwise weak password into a strong one.

Similarly, P22 "[does] not worry about security for the news account," so he used "two unrelated words (jungle and salmon) followed by digits" to create *junglesalmon711*. In the spectrum of passwords we observed for this study, "junglesalmon" is actually a relatively strong starting point because of the combinatorics of combining two unrelated words, yet P22 assumed it was weak because it contained dictionary words. To make a banking password, which he hoped would be strong, he prepended "R" and appended "@$" to the string he believed was insecure, expecting the resultant *Rjunglesalmon711@$* to be secure. As with P49, neither password was guessed by Hashcat; both are fairly secure. However, P22's misconception that minor changes to a password he believes is weak can make the password secure is troubling, especially when the capital letters and symbols are in predictable positions [38].

4.4.3 Algorithm for Password Creation

Most participants had an algorithm they always used to make a password. Rather than relying on reuse, these approaches followed conceptual patterns. For example, P3 always used a word, a year, and an emoticon. For low-security accounts, the word was a place she had visited. For high-security accounts, she used a "magic" word because she "want[s] it to be secure." Her resultant passwords were *Croatia2011:-p*, *Patagonia2014:-)*, and *HocusPocus;-)2003*. P7 always used words she associated with the site followed by a

single digit and an exclamation point. P19 stuck with a consistent order, "usually one capital, followed by lowercase letters, and a number or symbol."

In some cases, participants unwittingly created some passwords they believed to be strong and others they believed to be weak, yet the supposedly strong passwords were easier to guess. P35 was one such participant. As an English teacher, she liked to use "longer word[s]. It's what teachers expect from students, which is what made me think of it." Her algorithm was to add a digit onto a single long word. Her email and banking passwords, which she expected to be secure, were *Likelihood4* and *Deliberation9*. Both were guessed by Hashcat since "likelihood" and "deliberation" are in attackers' dictionaries, even if not in students' lexicons.

In contrast, she said, "I do not care about the security" for the news site and wanted to write "I journal." Because journaling is associated with newspapers, she said, "I think using a word related to the site would lessen the security." To make the word a little longer, she changed "journal" to "journalistic," resulting in the password *Ijournalistic?8*. This password, intended to be the weakest, was actually the strongest. While the participant associated the phrase "Ijournal" with a news site, this association is far from obvious.

In other cases, participants made passwords of similar strength despite expecting some to be far more secure than others. For example, none of P18's three passwords were guessed by Hashcat, yet she believed her news password was relatively weak and "simple" and her email and banking passwords were "really strong." Her approach to password creation was to pick words of significance to her and to write them in mnemonic form, usually followed by a symbol and some digits. The letters in her news password, *tdVc$567*, stood for "the da Vinci Code," while the letters in her email password, *Tjks&987*, represented the first names of her "siblings [and dog] in birth order." Her banking password, *_EmiLt345*, which she deemed to be the strongest, was based on the name of a "friend who lives out of the country," which is why she felt that password was strongest. However, all three passwords were strong; none were guessed by Hashcat.

Most participants said they developed their password-creation algorithm on their own, but 12 participants (24%) had read articles giving advice about creating secure passwords or attended an organizational security-training class. Unfortunately, both types of participants fell victim to misconceptions about security. P36, for example, had attended security training provided by her university and was taught to use phrases in passwords. As a result, in the study, she decided to use *ilove1sttrust!* as the password for the "First Trust National Bank." Although the participant believed this to be a "secure" password because it contained a phrase, "ilove" is a very common substring in passwords, and the name of the site, even slightly modified, is very predictable. The institutional security training, while correct in intent, fell short in helping P36 create secure passwords.

4.4.4 Order in Which Elements Are Chosen

One of the most common password structures when multiple character classes are required is a series of letters followed by a digit and a symbol [70, 71]. P44's approach was common among our participants: "I always put a capital letter at the beginning and numbers at the end."

Our think-aloud protocol let us unpack the order in which participants chose different elements of their passwords. We analyzed the order in which participants discussed each element of their password during its creation. The vast majority of participants first thought of a word, followed by digits and symbols. Their final passwords reflected this order.

For example, among passwords for banking accounts, which participants frequently deemed the most valuable, 29 participants created passwords containing letters, digits, and symbols. In 27 of these cases (93%), participants first chose the word they would use. In the remaining two cases, the participant first thought of the digit(s) they would use, followed by the word. Seventeen additional passwords contained letters and digits, but not symbols. For fifteen of these passwords (88%), the participant first chose the word; in only two cases did the participant first choose the number.

The consistency with which participants first chose a word to use, followed by digits and symbols, is particularly notable because for 82% of banking passwords, the order in which participants decided on elements is the order those elements appeared in their final passwords. In essence, the password is built from left to right as participants think of elements. Because passwords that begin with a word and end with digits and symbols are most common, one way to induce users to create stronger passwords might be to encourage them to scramble the elements of their password or, even better, to nestle digits and symbols into the middle of the words.

4.4.5 Password Management

Users' password-management strategies [18, 55] are central to their ability to use distinct, complex passwords for each account. We found that 17 of our 49 participants (35%) simply memorize their passwords without writing them down or storing them anywhere. For these participants, the memorability of the password is of paramount concern. In contrast, only two participants (4%) used a third-party password manager (KeyPass and LastPass, respectively), and only 6 participants (12%) used their browser to store passwords. Consistent with what prior research has shown [55], the remaining participants mixed memorization, writing passwords down, and storing passwords in ad-hoc ways on their computer.

A few participants had other considerations that impacted password creation. Two participants regularly reset their passwords, leading them to care greatly about the security of their email account. P29 uses a "family password" for her bank account to enable her parents to access it. As a result, she wants that password to be memorable to her parents, too.

4.5 Strategies and Misconceptions

Finally, we delve into micro-decisions participants made in the course of making a password. We documented micro-decisions through both the think-aloud protocol and the targeted questions in response to participants' behaviors and interview responses. We pay particular attention to participants' misconceptions.

As discussed in Section 3, our qualitative clustering of password-creation strategies enabled us to identify 122 distinct behaviors within the context of 25 broader themes. Table 3 presents the 25 broad themes we identified and how many of our 49 participants exhibited behaviors in each of those themes. As our analysis was purely qualitative, these counts should not be interpreted as generalizable to larger populations or comparable statistically. Instead, we provide these to give the reader a better sense of our data.

As shown in Table 3, we evaluated the security impact of each password-creation strategy based on the overall guessability of the passwords that employed that technique, as well as the frequency with which those techniques appear in passwords leaked in major breaches [21,48,60,62]. In some cases, different applications of the same strategy had very different impacts on security—sometimes beneficial and sometimes detrimental. For many passwords, however, the application of a particular strategy itself did not cause either a substantial increase of decrease in security. We do not explicitly call out these neutral impacts in the table.

Table 3: The categorization of participant strategies that resulted from our qualitative data analysis, along with how many participants (#) exhibited that behavior. Check marks denote that we observed instances of that behavior that made a password substantially *more* or *less* secure.

Categorization	#	More Secure	Less Secure
Choosing words/phrases (Section 4.5.1 and Section 4.5.2)			
Use a phrase	24	✓	✓
Use keyboard pattern for security	5		✓
Use non-English words for security	4	✓	✓
Use address or geographic location	10	✓	✓
Use names of family, friends, or pets	23		✓
Use information not on social media	5	✓	✓
Use uncommon dictionary word	11	✓	✓
Use word(s) inspired by the website	19	✓	✓
Base element is something participant likes	13	✓	✓
Base password on own workplace	5	✓	✓
Base password on pop-culture reference	11		✓
Password structure (Section 4.5.3)			
Create mnemonic	6	✓	✓
Intentionally non-standard capitalization	7	✓	
Capitalize first letters, following grammar	24		✓
Intersperse different character classes	6	✓	
Add string of "random" characters	9	✓	✓
Digits and symbols (Section 4.5.4)			
Replace letters with digits / symbols	14	✓	✓
Use information from bank card or ID card	3	✓	
Use date / year significant to self / family	17		✓
Other meaningful digits / symbols	24	✓	✓
Add symbol (usually "!") at end	18		✓
Expect symbol (e.g., "&") is hard to guess	16		✓
Meeting composition requirements (Section 4.5.5)			
Aim to make password longer than required	13	✓	
Explicitly include extra character classes	7	✓	
Feel any password meeting policy is secure	6		✓

The 25 broad themes we identified conceptually fit into four even broader approach areas. The first area, detailed further in Sections 4.5.1 and 4.5.2, centers on how participants chose the primary content, often semantically significant, that served as the foundation of the password. Usually after choosing this foundational content, participants imbued the password with additional structure (Section 4.5.3) through capitalization, mixing character classes, and added "randomness." Participants had varied strategies for using digits and symbols (Section 4.5.4) and meeting, or intentionally exceeding, the requirements of a password-composition policy (Section 4.5.5).

4.5.1 Choosing Words and Phrases

Choosing words to form the base element of a password was a crucial step in password creation. Our participants most often chose words based on personal topics (e.g., addresses, names, birthdays), associations to the site, their hobbies, nearby items, past events, keyboard patterns, work, and religion. As P23 explained, "I like to come up with words that mean something to me, something that I like, like the name of my favorite author, or a candy that I like to eat." Other participants used nearby objects for inspiration. For instance, P28 built her password around the product number of a camera on a shelf in our lab. Some participants correctly knew to avoid using their employer's name, their own name, their own birthday, or a single dictionary word. However, beyond these correct conceptions of high-level topics to avoid, participants fell victim to a number of misconceptions.

Many of these misconceptions were related to participants not understanding the automated nature of password-guessing attacks. They knew to avoid personal items about themselves, yet thought names and dates related to family members were fine. P6 structured her password around her name, yet placed a birthday (MMDD) in between her first and last name. She expected "a malicious person will try my birthday and my name, so I will not use my birthday...I will use...my pet dog's birthday." Unfortunately, automated attackers often try all possible birthdays rather than targeting a particular user's birthday [34,58,65]. Similarly, P7 built her password around the name of her dog, "Goldie." She expected "hackers cannot guess [it] because I have no pictures of him on my Facebook account." Although her dog's name is not on Facebook, it is a common pet name, making it a very likely target for attackers [60,64].

Misunderstandings about attackers also impacted the characteristics participants expected to be secure. For instance, P2 based his password around the Mahavishnu Orchestra, noting that he expected attackers would not be able to guess his password because "this band name is hard to spell." Because automated attackers use wordlists, words being hard to spell makes no difference for the attacker, only for the user. In crafting the password *purplep@nts*, P11 wanted to pick words that were secure, and she picked purple as "a color that is not often used, unlike red or white." Unfortunately, purple is just as common on word lists as are red and white.

Many participants had heard to avoid dictionary words in making passwords. As a result, P26 used the keyboard pattern *1Qazxsw2* as a password she intended to be secure. She said, "For online banking, I try to make my passwords a little more secure, so I like to follow a pattern on a keyboard." Similarly, P23 based the banking password she hoped would be secure around a keyboard pattern, which she mistakenly considered to be "random letters." Keyboard patterns are an easy target for automated attacks [54,60,64].

In contrast, other participants had developed approaches to word selection that resulted in much more secure passwords. For the banking website, P39 wanted to base his password around a song that he associates with money, and "the first song that comes to mind is Gold Digger. The phrase would be, 'I ain't saying she's a gold digger."' He transformed this phrase into a mnemonic and added three random characters. P4 similarly based her password, *$0.02CentShow*, on a music album that she associates with money. She chose to spell "2 cent" as "$0.02Cent" to be harder to guess. P28 created the complex password *LCiinf3-n*, explaining, "I usually create a sentence and take all the first letters," which is often considered good advice as long as the sentence is unique [36,49].

Other participants sadly undervalued the importance of choosing unique phrases when constructing a password. P17 chose the common aphorism "be the change" as the basis for one password, yet believed it to be secure because "someone wouldn't think [the phrase] necessarily applies to me." Similarly, P46 used a mnemonic of the famous opening line from *A Tale of Two Cities* ("It was the best of times, it was the worst of times") as the basis for her password. In contrast, P28 securely created a completely unique phrase to describe what was happening while she was creating a password.

A few participants crafted passwords that combined words from multiple languages, which may or may not be a secure strategy based on the languages and words chosen. For example, P6 used a Hawaiian word in her password, expecting its juxtaposition with English to be unpredictable. Other participants created strong passwords by combining unrelated words. P40 unintentionally created a reasonably secure password when he wanted to make a "short and simple" password for his low-value news account. He combined two unrelated words, "tossed in a few symbols," and appended "whooo" in crafting *Squ@shC2ndywhooo*.

4.5.2 Deriving Passwords from a Website

Using the website or service for which they were creating an account as inspiration was participants' second most common strategy after using personal names and dates. We found a sharp dichotomy of secure and very insecure instances of this strategy.

Many participants simply used the name of the site as a core component of their password, making such passwords easy targets for site-specific attacks. For instance, P36 had "heard that, instead of using words and numbers, using a phrase is more secure," so she created the password *Ilove1sttrust!* for the First Trust National Bank. Unfortunately, the name of the site is extremely predictable. Other participants used predictable word associations. For instance, P33 created the password *+Money369*. She used the word money "because it is a bank," and she used an increasing pattern on the number pad to represent an account balance she hoped would also be increasing.

In contrast, other participants used much more distant word associations in crafting far more secure passwords. These participants, like P38, avoided "the name of the service or the type of service because that would be too easy to guess." Many of these participants were inspired not just by the purpose of the site, but also the site's visual design (see Figure 1 in Section 3). For example, P13 said, "I saw the website logo picture and found a brown building on the left. So I used 'left' 'brown' as keywords followed by my favorite number and a symbol that looks like a building" in crafting *LEFTbrown8!* as his news password. Similarly, the news site logo reminded P32 of New York, which itself reminded her of "108." As a result, she created the password *newyorkONE008*, in which she added a 0 and mixed digits and capital letters for security. P39 used creative capitalization and uncommon punctuation to turn the lyrics from the Queen song "The Invisible Man" into a secure password. He chose this song as the basis for a secure email password "because I want the password to be invisible," using a distant association with the goal of the password as inspiration.

4.5.3 Capitalization, Punctuation, and Structure

As they decided how to integrate capital letters and other structures, many participants predictably capitalized the first letter of the password and added a single punctuation mark at the end. While in some cases participants said they did so out of laziness or simply because it is easy to remember, others said that years of schooling had inculcated the idea that capital letters come at the beginning and punctuation comes at the end. For example, P36 ended her password with an exclamation point "because that is how a sentence ends." These participants did not recognize that following the rules of grammar is detrimental to password security [47, 54, 60].

In contrast to the many participants who said they usually capitalize the first letter of passwords, some participants used far more creative approaches. For example, P13 crafted the password *8AX-Ewater<* based on the two items he associated with the job he had 8 years ago. He explained, "The security of an email account is important to me, so I capitalize some words and include a symbol that looks like an axe." The less predictable capitalization and less common symbol made his password stronger. Similarly, P31 knew to structure a password unpredictably, so he capitalized the "E" in *baldErdash49* "to randomize the password for security."

4.5.4 Use of Digits and Symbols

The most common, and most troubling, misconception we observed around the use of digits and symbols is that their inclusion automatically makes a password secure. We hypothesize this misunderstanding stems from advice that strong paswords contain digits and symbols (to increase the space of potential passwords) being misinterpreted as something akin to the assertion that including digits and symbols makes a password secure. Participants with this misunderstanding were well intentioned. For instance, P6 said, "I want to prevent others from predicting passwords, so I want to use all four types of [characters] for my password." Unfortunately, she did so in very predictable ways, with a capital letter at the beginning and a digit and a symbol at the end.

Many participants thought simply adding a symbol at the end of the password made it secure. As P45 said, "I added '!' at the end to make it secure." P34 felt that "usually numbers and a symbol will make the password strong." Therefore, he appended "24!" to each password, which otherwise were just the names of his three siblings. Users must be disabused of the notion that digits and symbols are a silver bullet for password security.

Years were common among participants' passwords. Unfortunately, years and dates are also well represented among top guesses by cracking tools [65]. Most of our participants did not seem to realize how predictable years are. For example, P49 made the password *Its1987* "because [he] was born in [that year]." Similarly, P25 appended "68" onto her full name to create her password because she was born in 1968. Perhaps even more predictably, P36 created the password *IloveNDT2014!* "since it's 2014."

Participants who used dates or years in their passwords commonly seemed to think only about threats from targeted attacks. For instance, P6 explained, "I think a malicious person will try my birthday and my name, so I will not use my birthday itself...I will use family information, such as my sister's birthday or my parents' birthday, or my pet dog's birthday." Compared to using her own birthday, P6's choices would give less of an advantage to an attacker in a user-specific attack, yet would do little to thwart a general attack.

Other choices of digits and symbols were more novel. Some participants used long sequences of digits and symbols that would be hard to predict. For instance, P9 used her student ID number from when she was in high school as the beginning of a password that was not guessed. In many other cases in which the digits or symbols were predictable, other parts of the password contributed enough unpredictability to make the password secure overall. P21 crafted *bAMBANG5$555*, combining his father's hometown with "5" because it "is a lucky number" and "$" "because it is a bank account." P42 also used the "dollar sign for money because this is a banking account." Her password, *ilovebillyC$1*, used the 1 at the end because Billy is her boyfriend and "he's number 1" in her book. A handful of other participants used digits to mirror meta-aspects of thir password. For instance, P46 included "2" in *Lethe+Styx27* because "there are two rivers (Lethe and Styx)" in the password, yet the "7" was random.

4.5.5 Meeting Requirements

One aspect where many participants came up short was deciding what to do when they did not meet a length requirement. The aforementioned transformation of "journal" into "journalistic" was a creative and accidentally effective approach of meeting a length requirement. In contrast, many participants simply tacked on a predictable number and symbol. Having decided to associate a piggy bank with the banking website, P8 came up with "pink piggy," yet found it was not long enough. Therefore, she added "1!," which is the most predictable ending for a password [60]. However, such predictable additions to a password have the added benefit of meeting digit and symbol requirements, which is why P2 said he always appends "1@." P49 found that "elephant" was not long enough and she said, "I don't want to choose another word," so she added numbers. This moment in password creation is ripe for a more thought-

ful intervention to help users make more creative, and hence less predictable, micro-decisions.

Other participants did not take full advantage of the tools at their disposal. For example, P1 is one of only two participants to use a password manager browser plugin, yet he reused the same weak password across all three accounts, which he said was typical of his behavior with his real accounts. Because his reused password ends with a three-digit "random number," he uses KeyPass to remember it. Instead, he would be far better served by using KeyPass to generate a unique, much harder to guess password for each account. Similarly, although P14 said that he writes his passwords down, he combined his sister's name and his initials into the password *jennlp1*, which was guessed in the general attack. Because he does not believe he can recall his passwords strictly from memory and thus plans to write the password down, he might be better served by making a less memorable, yet more secure, password.

5. DISCUSSION

Our participants' many misconceptions about passwords reveal that we, the community of password researchers and system administrators, are falling short in helping users understand how to make a secure password. We have become accustomed to shaming users for egregiously bad passwords [9, 35, 62]. However, we seem to have overlooked how to help motivated, well-intentioned users understand what precisely distinguishes a good password from a bad password, as well as what exactly they should be concerned about in the greater ecosystem of password security.

As a result, participants' folk models [68] about secure password behaviors often diverged from reality. In this section, we discuss directions for both improving the static advice given to users about password creation and designing interactive, data-driven tools to help users more intuitively understand why certain behaviors are predictable. These approaches aim to correct major misconceptions we identified in our qualitative data and thereby help users create secure passwords when they intend to do so.

5.1 Improving Advice About Passwords

We found that most of our participants have a human algorithm for generating their password. Some of these algorithms were generally secure, such as generating unique phrases that the participant associated with a site. In contrast, less secure algorithms often centered on reusing a base string with minor additions across accounts.

Summarizing good and bad behaviors for users can be difficult. We observed both secure and insecure variants of the same conceptal behaviors, and it is hard to capture nuances that distinguish them succintly. For example, participants who developed their password from an obscure song they associate with the website's logo were behaving securely. Those who made phrases like "ilove*SiteName*!" were not behaving securely despite also crafting a phrase related to the website.

5.1.1 Promoting Secure Human Algorithms

Security advice and requirements could focus on helping users develop and accurately judge human algorithms for developing passwords [49] rather than assuming the enforcement of a password-composition policy is sufficient. Password-composition policies often focus on character-class structures [29,33,56], rather than approaches and algorithms. A better approach might be to help users develop abstract approaches for generating passwords and accurately judge whether decisions they make are predictable.

For example, many participants expected that adding a digit or symbol to a password they considered weak would transform it into a secure password. These users seem to have misinterpreted canonical advice about including digits and symbols in passwords (on the assumption of increasing the password space) to be sufficient on its own for making a password secure. Abstract advice to "include digits and symbols" should be reworked to specify that these should be included randomly throughout the password. Tacking a digit or symbol onto the end of the password is not enough.

5.1.2 Assigning Value to Accounts

Participants' understanding and opinion of the relative value of accounts seemed surprisingly out of sync with what the security community might recommend. A rational user would make a simple password for all low-value accounts [48], such as accounts on news sites. Users should be reassured that "newspaper123" is actually a perfectly reasonble password for a low-value account; they should save their limited mental capacity for passwords for more important accounts [18,42]. We had expected email accounts, which can often be reused to reset passwords for other accounts, to be considered most valuable, followed by banking accounts. We expected accounts on news sites to be considered low-value. Only two of the 49 participants shared this appraisal, however, whereas 21 participants considered all accounts to be about the same value. Users need more guidance on how to make such value decisions so that they can reserve their effort for high-value accounts.

5.1.3 Understanding Threats

When explaining what makes a password insecure, participants mentioned targeted attacks using their own birthdays, names, addresses, and family members more frequently than attacks on abstract, yet predictable, behaviors. In essence, they were thinking of targeted attacks, rather than large-scale guessing. The community could better explain that both threats should be considered.

Furthermore, participants did not seem to understand automated guessing attacks. For example, the participant who expected that words that are harder to spell are harder for an attacker to guess is likely unaware of the mostly automated attacks [22] that take place when a password database is compromised [5,9,43,57]. Attackers are not typing candidate guesses; they are using word lists. Education efforts might build on Zhang-Kennedy et al.'s infographics helping users understand how password-guessing attacks work [73].

Participants also seemed to misunderstand the impact of password reuse on security. Reuse becomes problematic when an account is compromised and the attacker can then attack a high-value account with the same credentials. Thus, a user should have a set of distinct passwords for each of her handful of high-value accounts, whereas reuse is rational for low-value accounts [18].

5.2 Better Data-Driven Feedback

In concert with improved advice, interactive, data-driven tools could help correct users' misconceptions. In essence, data-driven approaches could help a user understand what everyone else does, pointing out the predictability of their own choices in crafting a password through examples.

We consistently observed that participants wanted different security levels for different sites, yet nonetheless crafted passwords of similar objective security or, in a few cases, more secure passwords for their intended lowest-value accounts. Currently, typical password-strength meters tell a user simply that their password is "very weak" or "very strong" based mainly on the password's length and number of character classes [15]. Large jumps in the password-security estimate by typical meters whenever a user adds an additional character class may have even contributed to the misconception that simply adding a digit or symbol to the end of a password greatly increases security. Instead, a data-driven feed-

back tool could leverage simulations of adversarial password cracking [31] to tell the user how long an attacker would take to guess that password. Similarly, tools could use large data sets of leaked passwords to help the user learn what patterns are predictable [32].

Participants seemed somewhat oblivious to the predictability and ubiquity of certain approaches, such as using a very common phrase as the basis for a password. Contrary to some participants' misconceptions, adding a "1" or "!" to the end of a password does not make it secure, and a famous quote is not a very good starting point for a password. Targeted, data-driven feedback during password creation could point out insecure behaviors that users seemed to think add security, yet might actually make a password weaker. The security misconceptions we note in this paper are a potential first set of detailed insecure behaviors to target. Such a tool could also point out the percentage of other users who employ such behaviors; leaked password sets could be used to bootstrap this tool.

Finally, we belive there is an opportunity for researchers to help users think of their password elements in unpredictable order and thereby craft passwords with less predictable structure. Participants often thought first of a word and then digits and symbols, thereby constructing their password in that (very common) order. One can imagine a tool that builds on prior work on persuasive tools [19] and automatically prompts users to think of password elements in a different order, or even automatically moves digits and symbols into unpredictable areas in the middle of the password.

6. CONCLUSION

We have reported on the first qualitative lab study of precisely how users construct passwords step-by-step. We found that many users have algorithms for developing passwords. Some of these algorithms are by and large secure, while others continually lead to passwords that are easy to guess. Many participants aimed to construct passwords of different security levels, yet the passwords they intended to be weak were often comparable to those they desired to be very strong. We also delved into participants' micro-decisions in constructing a password, finding numerous secure and insecure sources of inspiration for the words, phrases, digits, and structures they employ to craft a password. Building on participants' decisions and misconceptions, we have outlined directions for improving password guidance and designing data-driven tools to help users craft secure passwords for accounts they care about.

7. ACKNOWLEDGMENTS

This research was supported in part by NSF grants DGE-0903659 and CNS-1116776, and by a gift from Microsoft Research. This research was also conducted with government support under and awarded by DoD, Air Force Office of Scientific Research, via the National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a.

8. REFERENCES

[1] S. V. Acker, D. Hausknecht, W. Joosen, and A. Sabelfeld. Password meters and generators on the web: From large-scale empirical study to getting it right. In *Proc. CODASPY*, 2015.

[2] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[3] H. Beyer and K. Holtzblatt. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann, 1998.

[4] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. In *Proc. USEC*, 2015.

[5] J. Bonneau. The Gawker hack: How a million passwords were lost. *Light Blue Touchpaper* Blog, December 2010. **http://www.lightbluetouchpaper.org/2010/12/15/the-gawker-hack-how-a-million-passwords-were-lost/**.

[6] J. Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *Proc. IEEE Symposium on Security and Privacy*, 2012.

[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. In *Proc. IEEE Symposium on Security and Privacy*, 2012.

[8] J. Bonneau and E. Shutova. Linguistic properties of multi-word passphrases. In *Proc. USEC*, 2012.

[9] J. Brodkin. 10 (or so) of the worst passwords exposed by the LinkedIn hack. *Ars Technica*, June 2012.

[10] W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. Technical report, NIST, 2006.

[11] D. Cameron. Apple knew of iCloud security hole 6 months before Celebgate. *The Daily Dot*, September 24 2014. **http://www.dailydot.com/technology/apple-icloud-brute-force-attack-march/**.

[12] C. Castelluccia, M. Dürmuth, and D. Perito. Adaptive password-strength meters from Markov models. In *Proc. NDSS*, 2012.

[13] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle. Multiple password interference in text passwords and click-based graphical passwords. In *Proc. CCS*, 2009.

[14] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *Proc. NDSS*, 2014.

[15] X. de Carné de Carnavalet and M. Mannan. From very weak to very strong: Analyzing password-strength meters. In *Proc. NDSS*, 2014.

[16] S. Fahl, M. Harbach, Y. Acar, and M. Smith. On the ecological validity of a password study. In *Proc. SOUPS*, 2013.

[17] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proc. WWW*, 2007.

[18] D. Florencio, C. Herley, and P. C. van Oorschot. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proc. USENIX Security*, 2014.

[19] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In *Proc. SOUPS*, 2008.

[20] S. Gaw and E. W. Felten. Password management strategies for online accounts. In *Proc. SOUPS*, 2006.

[21] D. Goodin. Hackers expose 453,000 credentials allegedly taken from Yahoo service. *Ars Technica*, July 2012. **http://arstechnica.com/security/2012/07/yahoo-service-hacked/**.

[22] D. Goodin. Why passwords have never been weaker—and crackers have never been stronger. *Ars Technica*, August 2012. **http://arstechnica.com/security/2012/08/passwords-under-assault/**.

[23] D. Goodin. Anatomy of a hack: How crackers ransack passwords like "qeadzcwrsfxv1331". *Ars Technica*, 2013. **http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/**.

[24] D. Goodin. "thereisnofatebutwhatwemake"-turbo-charged cracking comes to long passwords. *Ars Technica*, August 2013. **http://arstechnica.com/security/2013/08/thereisnofatebutwhatwemake-turbo-charged-cracking-comes-to-long-passwords/**.

[25] Google. Web 1T 5-gram version 1, 2006. **http://www.ldc.upenn.edu/Catalog/CatalogEntry.jsp?catalogId=LDC2006T13**.

[26] Google. 2-step verification. **https://www.google.com/landing/2step/**, 2015.

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

[28] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proc. NSPW*, pages 133–144, 2009.

[29] P. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. In *Proc. CHI*, 2010.

[30] M. Jakobsson and M. Dhiman. The benefits of understanding passwords. In *Proc. HotSec*, 2012.

[31] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Proc. IEEE Symposium on Security and Privacy*, May 2012.

[32] S. Komanduri, R. Shay, L. F. Cranor, C. Herley, and S. Schechter. Telepathwords: Preventing weak passwords by reading users' minds. In *Proc. USENIX Security*, 2014.

[33] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Proc. CHI*, 2011.

[34] KoreLogic. "Crack Me If You Can" - DEF CON 2010. **http://contest-2010.korelogic.com/rules.html**, 2010.

[35] L. Kornblatt. When "most popular" isn't a good thing: Worst passwords of the year – and how to fix them. **http://www.splashdata.com/press/PR111121.htm**, November 2011.

[36] C. Kuo, S. Romanosky, and L. F. Cranor. Human selection of mnemonic phrase-based passwords. In *Proc. SOUPS*, 2006.

[37] D. Love. Apple on iCloud breach: It's not our fault hackers guessed celebrity passwords. *International Business Times*, September 2 2014. **http://www.ibtimes.com/apple-icloud-breach-its-not-our-fault-hackers-guessed-celebrity-passwords-1676268**.

[38] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur. Measuring password guessability for an entire university. In *Proc. CCS*, 2013.

[39] B. D. Medlin and J. A. Cazier. An empirical investigation: Health care employee passwords and their crack times in relationship to hipaa security standards. *IJHISI*, 2(3), 2007.

[40] Microsoft. About two-step verification. **http://windows.microsoft.com/en-us/windows/two-step-verification-faq**, Accessed 2015.

[41] D. A. Milman. Death to passwords. ComputerWorld. **http://blogs.computerworld.com/17543/death_to_passwords**, 2010.

[42] R. Nithyanand and R. Johnson. The password allocation problem: Strategies for reusing passwords effectively. In *Proc. WPES*, 2013.

[43] N. Perlroth. Adobe hacking attack was bigger than previously thought. *The New York Times Bits Blog*, Oct. 2013. **http://bits.blogs.nytimes.com/2013/10/29/adobe-online-attack-was-bigger-than-previously-thought/**.

[44] PHDays. "Hash Runner" - Positive Hack Days. **http://2013.phdays.com/program/contests/**, 2013.

[45] R. W. Proctor, M.-C. Lien, K.-P. L. Vu, E. E. Schultz, and G. Salvendy. Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers*, 34(2):163–169, 2002.

[46] N. Provos and D. Mazieres. A future-adaptable password scheme. In *Proc. USENIX ATC*, 1999.

[47] A. Rao, B. Jha, and G. Kini. Effect of grammar on security of long passwords. In *CODASPY*, 2013.

[48] B. Schneier. MySpace passwords aren't so dumb. **http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300**, 2006.

[49] B. Schneier. Password advice. **www.schneier.com/blog/archives/2009/08/password_advice.html**, August 2009, retrieved September 2012.

[50] SCOWL. Spell checker oriented word lists. **http://wordlist.sourceforge.net**, 2015.

[51] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor. Can long passwords be secure and usable? In *Proc. CHI*, 2014.

[52] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: Implications for security design based on social practice. In *Proc. CHI*, 2007.

[53] F. Stajano. Pico: No more passwords! In *Proc. SPW*, 2011.

[54] J. Steubbe. Hashcat. **http://hashcat.net/oclhashcat-plus/**, 2009.

[55] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Proc. SOUPS*, 2014.

[56] W. C. Summers and E. Bosworth. Password policy: The good, the bad, and the ugly. In *Proc. WISICT*, 2004.

[57] Trustwave. eHarmony password dump analysis, June 2012. **http://blog.spiderlabs.com/2012/06/eharmony-password-dump-analysis.html**.

[58] Trustwave Spiderlabs. SpiderLabs/KoreLogic-Rules. **https://github.com/SpiderLabs/KoreLogic-Rules**, 2012.

[59] B. Ur, P. G. Kelly, S. Komanduri, J. Lee, M. Maass, M. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. How does your password measure up? The effect of strength meters on password creation. In *Proc. USENIX Security*, August 2012.

[60] B. Ur, S. Komanduri, R. Shay, S. Matsumoto, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, M. L. Mazurek, and T. Vidas. Poster: The art of password creation. In *Proc. IEEE Symposium on Security and Privacy*, 2013.

[61] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay. Measuring real-world accuracies and biases in modeling password guessability. In *Proc. USENIX Security*, 2015.

[62] A. Vance. If your password is 123456, just make it HackMe. New York Times, **http://www.nytimes.com/2010/01/21/technology/21password.html**, 2010.

[63] A. Vance, D. Eargle, K. Ouimet, and D. Straub. Enhancing password security through interactive fear appeals: A web-based field experiment. In *Proc. HICSS*, 2013.

[64] R. Veras, C. Collins, and J. Thorpe. On the semantic patterns of passwords and their security impact. In *Proc. NDSS*, 2014.

[65] R. Veras, J. Thorpe, and C. Collins. Visualizing semantics in passwords: The role of dates. In *Proc. VizSec*, 2012.

[66] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, and J. Cook. Improving password security and memorability to protect personal and organizational information. *IJHCS*, 65(8):744–757, 2007.

[67] C. Warner. Passwords with simple character substitutions are weak. **http://optimwise.com/passwords-with-simple-character-substitution-are-weak/**, 2010.

[68] R. Wash. Folk models of home computer security. In *Proc. SOUPS*, 2010.

[69] M. Weir. The RockYou 32 million password list top 100. **reusablesec.blogspot.com/2009/12/rockyou-32-million-password-list-top.html**, December 2009, retrieved September 2012.

[70] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proc. CCS*, 2010.

[71] M. Weir, S. Aggarwal, B. d. Medeiros, and B. Glodek. Password cracking using probabilistic context-free grammars. In *Proc. IEEE Symposium on Security and Privacy*, 2009.

[72] Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proc. CCS*, 2010.

[73] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *Proc. eCRS*, 2013.

APPENDIX

A. INTERVIEW SCRIPT

Good {morning, afternoon}. My name is _____ and I will be moderating your interview today. First, I would like you to review this consent form. It contains important information about today's interview. If you consent to the terms and would like to participate in the study, please sign the form and hand it back to me.

Today, we will be asking you questions that relate to how you create passwords. You are free to choose not to answer any questions, and to stop the interview at any point if you feel uncomfortable. We will ask you to create new passwords as if you were creating them for certain services. Please note that we will not ask you to tell us your passwords you use for the services you are currently signed up for in your real life. We greatly value your honest and candid responses.

Later in this session, we would like to make an audio recording of this session. This recording will only be used for the purposes of this study and will only be accessible to the researchers. Do you consent to having this session audio recorded?

First, I would like to ask you about yourself.

Demographics

1. How old are you?
2. What is your nationality?
3. What is your gender?
4. What is your occupation?
5. (If relevant from the answer to the previous question) What is your {role, expertise, major} in your occupation?
6. What is the highest level of education that you have completed?
7. Please rate your computer skills and knowledge from 1 to 5, with 1 being the lowest and 5 being the highest?
8. For how many hours a day on average do you use the Internet?
9. Do you use your own computer, or a shared computer, when using the Internet?
10. What kind of computer devices do you use? (PC, smart phone, tablet, etc.)
11. (If answer to the question 10 includes a smart phone) What kind of smart phone do you use?

Now, let me start recording audio.

12. What is the purpose of using the Internet on your device(s)? What kinds of websites do you visit?
13. (If the participant has multiple devices) When using the Internet, do you use all the devices for the same purposes at the similar frequency, or do you use them differently?
14. (If the answer to the question 13 is "differently") Why do you use those devices differently when using the Internet? Do you think one device is more secure than others? Other reasons?
15. Do you need to type in a password for any of the Internet services on your device(s)?
16. What kind of Internet services have you signed up for?

Password Creation

Thank you. Now, I am going to ask you to create new passwords for 3 different types of services.

You will be asked to type the passwords in the password field on the computer. While creating the passwords, we will ask you to "think aloud" to help us understand what your password-creation strategy is.

Please listen carefully to the example of "thinking aloud" I am going to give you, and please follow the same method when you create new passwords.

> I am thinking aloud to design an anti-drunk driving bumper sticker as an example. Now let's see.., I'll start with the colors I will be using. One of the colors I will use is red because it symbolizes both warning and blood. I thought of blood because drunk driving may cause accidents that involve injuries or deaths. And for the design... hmm, well, I want to use something like the no-smoking sign, that is, a red circle with backslash, and... let's place something that represents alcohol behind it.... say, a beer bottle, because it is very straightforward at a glance. And having a beer bottle placed behind a red circle with the backslash would be, uh, pretty easy to understand that it means alcohol beverages are prohibited. Hmm, actually, should I use a can or bottle? Um, I think I will stick with a beer bottle, because a beer can may look like a soda can. Hmm, and the background color should be definitely white because it would make the symbol stand out more. I will also put "Don't drink and drive" on the right hand side of the symbol using a big font, uhh, probably in green because it is an opposite color to red, so along with the red symbol, I think it will make the sticker look really striking. Oh, and I will put an exclamation mark at the end of the sentence, because it would give us impression of urgency and importance.

Now, we are going to ask you to use the same thinking-aloud process when you create passwords. Again, please do not use the same passwords you are currently using for any of your real accounts. Please pretend that you are actually creating new passwords to sign up for new services, and remember to say aloud what exactly you are thinking when doing so. Please create a password in the same way you would if this were your real password and you need to use those passwords again to log in to the account you sign up for. In addition, please take the steps you would normally take to remember your password and protect this password as you normally would protect the password for this type of account. For example, if you normally write down this type of password, you should go ahead and do that. Please behave as you would if this were your real password! After you finish creating your passwords for this study, we're going to have you do some tasks to clear your mind, and then we're going to have you try to log in again using the password you created. So keep that in mind as you create your password. Please also explain the reason for choosing a certain words or characters, for example, please say "I will choose 1 as a numerical character because it is easy to remember," instead of just "I will choose 1 as a numerical character." Also please note that I may ask you for a clarification for the reason you chose certain words or characters.

You are asked to create 3 passwords for different type of services and those are free news subscription, email, and online banking services. All of your passwords must follow a certain composition rule.

You will be asked to create your new passwords starting at the next step, but please do not start typing a password until I ask you to do so.

Please click continue.

Password for of News/Email/Bank
Now, please pretend that you are creating a new password to {log into a free newspaper website such as NY Times, CNN, etc. | sign up for an email account such as Gmail, Hotmail, etc. | sign up for an online banking service}. Again, while creating password, say aloud exactly what you are thinking, as in the example I gave you. Please do not click continue until I ask you to do so. Please use the computer and start typing in the password you create as you explain your thinking process.

After confirming the thinking aloud process
Thank you. Please click continue and do not start typing until I ask you to do so.

Password for News/Email/Bank
Now, please pretend that you are creating a new password to {log into a free newspaper website such as NY Times, CNN, etc. | sign up for an email account such as Gmail, Hotmail, etc. | sign up for an online banking service}. Again, while creating password, say aloud exactly what you are thinking, as in the example I gave you. Please do not click continue until I ask you to do so. Please use the computer and start typing in the password you create as you explain your thinking process.

After confirming the thinking aloud process
Thank you. Please click continue and do not start typing until I ask you to do so.

Password for News/Email/Bank
Now, please pretend that you are creating a new password to {log into a free newspaper website such as NY Times, CNN, etc. | sign up for an email account such as Gmail, Hotmail, etc. | sign up for an online banking service}. Again, while creating password, say aloud exactly what you are thinking, as in the example I gave you. Please do not click continue until I ask you to do so. Please use the computer and start typing in the password you create as you explain your thinking process.

After confirming the thinking aloud process
Thank you. Please click continue and please do not click anything until I ask you to do so.

Now, please answer a few additional questions related to your password-creation strategy.

17. What is the first thing on your mind that comes up when creating a password? (If clarification requested: Is it a digit, keyword, something that associates the type of services, or something else?)
18. How do you pick your keywords? Are they related to your hobbies, what you find in your room, or something else?
19. Could you tell me what process you go through to select what you use for your passwords? (If clarification requested: For example, you can say "First, I pick up a favorite song, and then a songwriter. Then I choose a number associated with the song like a released year," etc.)
20. What aspect of your password do you think make the password harder to crack?

Password Challenges

21. As far as you know, have any of your Internet service account passwords been stolen or leaked?
22. (If answer to the question 21 is yes) Did it cause you to change anything about the way you create passwords? How?
23. Was your password creation strategy in our study today different from the way you create passwords normally?
24. (If the answer to the question 23 is yes) How different was it, and why?

25. When was the last time you created a new password before the study? You may answer by rough estimate.
26. What strategy did you use to create the password you created last time? Was it different from the one you used today?
27. How did you come up with the strategy you used today (and you use normally)?
28. (If the passwords contain a number or symbol) How did you come up with the number/symbol you used today?
29. Have you ever reused any of your passwords exactly as they are before?
30. Why? / Why not?
31. Have you ever reused a part of any of your passwords before?
32. Why? / Why not?
33. (If the answer to question 29 or 31 is yes) Do you reuse your passwords rarely, always, often or only occasionally?
34. (If the answer to question 29 or 31 is yes) When are you likely to reuse your password and why?
35. (If the answer to question 29 or 31 is yes) When are you not likely to reuse your password and why?
36. (If the answer to the question 31 is yes) Would you explain how you modify existing password for reuse?
37. Are you concerned about the security of reusing passwords?
38. (If the answers to both question 29 or 31 and 37 are yes) Then why did you reuse your passwords?
39. Some passwords are required to be changed periodically, like every 90 days. Have you changed a password for an existing account because you are required to change it periodically? If yes, what was the strategy you used to change the password? Did you create a whole new password or modify the old password?

Thank you.

Distraction Task
Now, I am going to ask you to do some simple task. This task is not related to passwords, so you can relax and take your time to finish it. Please count backwards from 100 in sevens, that is, starting from 100, subtract 7 from each number you say, like 100, 93, and so on.

Now, recall you created 3 new passwords during the first session. You will be asked to enter the passwords you created to see if you remember them correctly. For this session, please think aloud again to help me understand how you are remembering your password. Please note that the type of service shown on the screen may be in a different order from the one you saw when you created your passwords.

You can click the continue button on the screen to start entering the password. You are allowed to make up to 5 attempts per password.

Remembering {News/Email/Bank} Password
Please enter the password you created for the {News/Email/Bank} account, and while doing so, please think aloud again how you are remembering your password. Please click continue to see if you remembered it correctly or not.

40. If they did not remember the password in 5 times: Why do you think you had a problem remembering the password?

Remembering {News/Email/Bank} Password
Please enter the password you created for the {News/Email/Bank} account, and while doing so, please think aloud again how you are remembering your password. Please click continue to see if you remembered it correctly or not.

41. If they did not remember the password in 5 times: Why do you think you had a problem remembering the password?

Remembering {News/Email/Bank} Password
Please enter the password you created for the {News/Email/Bank} account, and while doing so, please think aloud again how you are remembering your password. Please click continue to see if you remembered it correctly or not.

42. If they did not remember the password in 5 times: Why do you think you had a problem remembering the password?
43. How do you usually remember your passwords? Do you store it electronically, such as using a password manager, or write it down on paper?
44. (If the answer to 43 is electronically) Which tool do you use to store passwords?
45. (If the answer to 43 is paper) Where do you write it down? Do you look at it every time you have to enter it or do you try to to remember it first?
46. How hard do you think it would be for your friends or family to guess your password? If a cybercriminal were to compile a list of the most common passwords, do you think your password would be on it? What if that list was compiled by the government?
47. Is there anything else about password creation strategy you used you think is useful for us to know about how you create passwords?

Interview Conclusion
Thank you very much for participating! Your feedback has been valuable to our research. We will eventually write a research paper about conversations we are having with you and a number of other research participants. In the research paper, we would like to include quotes from some of our participants, attributing these quotes to "Participant #."

47. Do you give us your permission to use quotes from you in this research paper?
48. Are there any things we discussed today that you would like us to not quote?

Thanks again!
Compensates participant.