The Password Life Cycle

ELIZABETH STOBERT and ROBERT BIDDLE, Carleton University

Managing passwords is a difficult task for users, who must create, remember, and keep track of large numbers of passwords. In this work, we investigated users' coping strategies for password management. Through a series of interviews, we identified a "life cycle" of password use and find that users' central task in coping with their passwords is rationing their effort to best protect their important accounts. We followed up this work by interviewing experts about their password management practices and found that experts rely on the same kinds of coping strategies as non-experts, but that their increased *situation awareness* of security allows them to better ration their effort into protecting their accounts. Finally, we conducted a survey study to explore how the life cycle model generalizes to the larger population and find that the life cycle and rationing patterns can be seen in the broader population, but that survey respondents were less likely to characterize security management as a challenging task.

CCS Concepts: • **Security and privacy → Usability in security and privacy**;

Additional Key Words and Phrases: Authentication, usable security, coping strategies

ACM Reference format:
Elizabeth Stobert and Robert Biddle. 2018. The Password Life Cycle. *ACM Trans. Priv. Secur.* 21, 3, Article 13 (April 2018), 32 pages.
https://doi.org/10.1145/3183341

1 INTRODUCTION

Passwords present many difficult tasks for users. Users are told to create strong passwords, not to reuse passwords on multiple accounts, and not to write their passwords down. Yet users have many passwords and are expected to create a password for every new service. Often, users are required to change their passwords at regular intervals. Taken as a whole, these requirements are difficult, if not impossible, for users to meet, and in response, users develop strategies for coping as best they can. In this work, our goal was to explore and understand these strategies in the hope of identifying new ways to alleviate the difficulties.

In this work, we developed, triangulated, and validated a cyclic model of password reuse. We interviewed users to find out about their password coping strategies. We asked how many accounts and passwords they have, how they create and reuse passwords, and how they handle password changes. We encouraged participants to discuss their experiences in rich detail and share their motivations, fears, and password tricks.

This work was supported by the National Science and Engineering Research Council of Canada through a Canada Graduate Scholarship, and funding from NSERC ISSNet.
Authors' addresses: E. Stobert and R. Biddle, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6; emails: {elizabeth.stobert, robert.biddle}@carleton.ca.

https://doi.org/10.1145/3183341

We used the Grounded Theory methodology to elicit a comprehensive theory of password reuse. Although it has been known that users reuse passwords, our goal was to understand the complexity of ways in which users reuse passwords, why they do so, and to fit this understanding into a larger pattern of behaviour. Grounded Theory is a qualitative analysis technique that "*construct[s]* from data an explanatory scheme that systematically integrates various concepts through statements of relationship" [41, p. 25]. Although a variety of studies have discovered specific elements of password reuse, ours is the first work to systematically interrelate these behaviours and theorize about the underlying phenomenon. We wished to gain insight into the rich detail of peoples' experiences in managing passwords, and we explored these details by fostering a supportive environment, by encouraging detailed discussion, and by providing props to help users situate themselves in the scenarios we were exploring.

Some findings were unsurprising. Users do write passwords down and do reuse passwords. However, these are simplifications of their actual behaviour that do not tell the whole story. For example, users often write down passwords as a fallback strategy, and when they reuse passwords, they frequently adapt them for different accounts. We identified a "life cycle" of password use, where the user's central concern is rationing effort to best protect important accounts. Many of the specific practices are already known, and our contribution is the identification of a coherent model that highlights a consistent series of gaps between user behaviour and current tool support. We describe the emergence of this model and suggest that it can inform better ways to support users in their behaviour.

Following up our initial study of non-expert users, we triangulated the theory in a series of interviews with computer security experts. Using the codes from the first study, we found that experts displayed many of the same coping strategies as non-experts. We conducted a new thematic analysis to understand what benefits are bestowed on knowledgeable users by their expertise and how this helps them handle the demands of passwords. Finally, to investigate how our life cycle model generalizes to a larger population, we developed a survey instrument based on the results of the life cycle model and distributed it to about 350 participants. We found that the patterns of the life cycle and rationing can be seen in the wider population, but that the survey respondents were less negative about the burdens of passwords on their lives.

2 BACKGROUND

Passwords pose a considerable usability challenge for end users, who are asked to create secure, unique passwords for every account, remember each of those passwords for a long time, and remember which password goes with which account for multiple accounts. These security requirements place demands beyond human capability on users' memory, time, and attention [20] and lead users to create passwords that are memorable but easily guessed by attackers. This is known as the password problem [48]: Passwords that are easy to remember are also easy to guess.

The password problem has existed for most of the history of computing. Morris and Thompson describe the problem in a 1979 article about passwords in the Unix operating system. However, with the introduction of personal computing and the web, the problem has scaled enormously. Current research continues to find users creating weak passwords [8], and instances of leaked or stolen passwords leading to major losses are increasingly common. The password problem results from a mismatch between security expectations and users' abilities [48], and these disconnects can lead to the misuse or avoidance of security mechanisms [1]. Users often behave against expectations by writing passwords down or by reusing the same passwords across multiple accounts.

Deployed solutions to the password problem consist mainly of password managers, which store and enter users' passwords, thus saving the user from remembering their passwords or which passwords are associated with which accounts. Browser-based password managers save passwords

when they are typed into the appropriate fields and then automatically input them when the page is visited again (often without authentication). Dedicated password managers (such as LastPass [28]) typically store the user's passwords in a password "wallet" that is protected by a master password (which may be required at every login).

Existing research on password managers has shown that they can have usability problems that affect their ability to securely manage users' passwords. A 2006 study of two password managers found that both managers had significant usability issues [11]. Worse, participants had poor mental models for how the software worked, and these poor mental models led them to make dangerous and unrecoverable security errors.

Another solution to the password problem is single sign-on, where one party authenticates users for multiple websites. At login, the user presents their credentials to the authenticating party, who checks the credentials and relays the results to the website. A study of the OpenID single sign-on protocol [42] found that adoption was hindered because it did not fit into users' existing password management techniques, and users were concerned about trusting a single entity to log into multiple sites.

2.1 Password Use

Several studies have investigated the number of passwords and accounts possessed by users. Gaw and Felten [21] found that undergraduates had an average of about 12 accounts, but they had fewer unique passwords and password reuse was rampant. The study also found that most participants cited easier memorability as their reason for password reuse, and that participants classified their accounts by the desired level of privacy and security. Florencio and Herley [19] conducted a large-scale study of password use through the 6-month deployment of a Microsoft toolbar. They collected data from more than 250,000 users and found that the average user had 6.5 passwords, each of which was shared across 3.9 websites. They found that the average user accessed 25 accounts over the 6-month period, and logged into eight accounts per day. A diary study of password use by Hayashi and Hong [23] collected detailed records of password entries over a 2-week period. They found that users accessed a mean of 8.6 accounts over 2 weeks and estimated that most participants had about 11 accounts in total. Although they did not study password reuse directly, all of their participants reported reusing passwords across multiple accounts. A more recent diary study [38] conducted in an organizational setting found that users authenticated 23 times a day on average and were frustrated by the frequent disruptions to their primary tasks.

While several studies have investigated *what* users do to cope with passwords, there exists less investigation into *why* users behave the way they do. Wash [45] identified folk models of security threats (viruses and malware) that users use to justify ignoring security advice. A follow-up study [33] investigated how users find information about security and found that most users depend on informal shared security stories from friends and family.

2.2 Coping Strategies

Conventional wisdom assumes that users are lazy and unwilling to comply with security advice. Correspondingly, the conventional suggestion is that users should be motivated to try harder to follow security advice and be better educated about the dangers of poor security practices. However, the quantity of information is arguably impossible for users to memorize [20]. Users often end up ignoring security advice, and Herley [24] argues that these decisions are rational. Not only are password expectations impossible for users to meet, but a cost–benefit analysis of following security advice suggests that users should not even try.

2.2.1 Reusing Passwords. One technique for coping with the demands of multiple passwords and accounts is to reuse passwords across multiple accounts. Reusing passwords carries security risks because an attacker may be able to uncover a password for one website and then use that password to attack a user's other accounts (e.g., through the leak of a password database). In spite of these risks, many studies have uncovered password reuse [19, 21, 23, 31, 36, 39, 49]. Notoatmodjo [31] found that reuse increased with the number of users' accounts and that most users cited increased memorability as the reason for reusing passwords. Reuse is a simple and intuitive coping technique that scales well to handling password meters [14] and coping with password policies [36].

Empirically tracing the extent of password reuse can be difficult. Das et al. [12] examined leaked datasets from 10 websites and found that 43% of all passwords in their dataset were reused across multiple accounts. Wash et al. [46] tracked password use through a browser extension and found that people tend to reuse passwords on between 1.7 and 3.4 websites.

Even when users do not completely reuse passwords, they often reuse pieces of passwords, or make minor modifications when using a password on another website. Most transformations take place at the beginning or end of a password, and the most common transformations are to add a number, symbol, or capitalization to comply with a new password policy [12, 43, 47]. Users often retain fragments of existing habits and passwords across the creation of new accounts and changes in policy, leading to long-term reuse [44].

2.2.2 Writing Passwords Down. Another coping strategy that users adopt for remembering passwords is to write passwords down. Writing passwords down can allow users to select and remember more complex passwords, as well as a higher number of passwords, but can have security risks if an attacker were to discover the recorded list.

Many users write down some or all of their passwords. Zviran and Haga [49] asked users about their password recording practices and found that 35% of their participants wrote down their passwords, and the most common storage locations for recorded passwords were wallets, notebooks, and calendars. An important issue for recorded passwords is how they are stored: If securely stored, writing passwords down can be a perfectly acceptable technique for aiding users with passwords. Shay et al. [36] asked users how they protected their recorded passwords and found that about 30% of people did not protect them at all. Of the remaining 70%, strategies were varied but included hiding the list of passwords or storing it on another computer or device with a password.

2.3 Security Practices of Experts and Non-Experts

Quite a lot of work has focused explicitly on non-expert users. Wash [45] investigated non-experts' mental models of security and found that users have often inaccurate folk models of viruses and hackers that affect how users perceive and react to threats.

Work comparing experts with non-experts has generally found that experts focus on different parts of the problem than non-experts. Asgharpour, Liu, and Camp [6] had experts and non-experts participate in a card-sorting experiment to elicit mental models of security. They found that expert users' mental models of security differed from those of non-experts and that a physical security metaphor was likely to be useful for framing computer security messages. Kang et al. [26] investigated users' mental models of the internet and examined perceptions of security and privacy online. Their results showed that both technical and non-technical participants suffered from high levels of uncertainty around how information is collected and shared online. Although technical participants had different concerns, all were somewhat affected by not knowing how to handle the problems. Ion, Reeder, and Consolvo [25] examined the security practices of expert users in a survey-based study. They examined exclusive practices of experts vs. non-experts and found

that experts were likely to mention "unique" passwords and the use of password managers, while non-experts discussed "strong" passwords and password change policies. Stobert and Biddle [40] found that experts report many of the same difficulties and coping strategies for passwords as non-experts.

Norman [30] reports anecdotal evidence that experts reuse and record passwords to handle the difficulty of remembering secure passwords. He reported that many security professionals told him that they reused two passwords: a strong password and a weak password. For accounts with unusual password requirements, they reported writing passwords down.

3 STUDY 1: HOW DO END USERS COPE WITH PASSWORDS?

The goal of our first study was to conduct a principled investigation into how end users cope with password management. We were interested not only in what participants did but also why they did it.

3.1 Method

To investigate how users manage and keep track of their passwords, we conducted a series of semi-structured interviews about password habits. We conducted the interviews ourselves, which included asking the questions, recording answers, and encouraging participants to discuss or give fuller answers. The interviews were audio recorded to allow further note-taking and analysis. We also conducted a brief self-administered demographics questionnaire that collected basic information including age, gender, and occupation and was mostly intended to give a better understanding of the interview sample. The study was approved by the Carleton University Research Ethics Board.

We developed our interview questionnaire around the idea of exploring users' password management techniques. We asked a set of general questions about password habits and usage, including questions about how many passwords and accounts participants had, whether they reused passwords, whether they used password managers, and how they kept track of their passwords. The next series of questions asked about how they would behave when creating new accounts, and when changing or resetting the password on an existing account. We did not ask participants what their passwords were, and we specifically told participants that they should never reveal their passwords to us. We used the Grounded Theory constant comparative approach [41] when conducting the interviews, where we refined the focus of the interview discussion throughout the study. Each interview took approximately 30 minutes, and the interviews were conducted at Carleton University.

We chose our methodology to encourage participants to thoughtfully discuss the ways in which they approach the task of password management. We used a guided interview to focus the discussion around topics of interest to us, but we asked additional questions to probe responses and follow up on emerging topics of interest. We broke questions into a number of parts to give participants an opportunity to fully explain how and why they make their decisions and to avoid having participants rush through their answers. We provided users with props in the form of cards with website screenshots (Figure 1) to situate themselves in the password creation and reset tasks, and to encourage them to consider their real-life behaviour. We carefully fostered a supportive and non-judgmental environment in the interviews, assuring users that their experiences were valid and of interest and that our purpose was not to disparage poor security practices.

We used Grounded Theory [41] to analyze the interview data and conduct qualitative analysis of participants' responses and discussion. Grounded Theory is an analytical framework that seeks to develop an explanatory theory from a set of qualitative data. It builds a theory grounded in

Fig. 1. Participants were provided with cards showing website screenshots. The purpose of these cards was to let participants better immerse themselves in the interview questions by imagining that they were creating an account on the pictured websites. The cards also provided a shared reference for the discussion, inviting deixis and physical interaction.

evidence rather than validating an outside theory or testing generalizability. Grounded Theory defines a theory as

> ...a set of well-developed categories (e.g., themes, concepts) that are systematically interrelated through statements of relationship to form a theoretical framework that explains some relevant social, psychological, educational, nursing, or other phenomenon. [41, p. 22]

The goal of Grounded Theory is to establish an explanatory theory that identifies the underlying phenomenon causing observed patterns. Grounded Theory is an established methodology that has been widely applied in usable security [1, 2, 4, 13, 27, 29].

In addition to the deeper responses and discussion, the interviews also yielded a set of numerical responses to the questions about how many passwords and accounts users have, how many passwords they reuse, and the extent to which they use password managers and other tools. Before presenting the Grounded Theory analysis in Section 3.3, we present a quantitative overview of the descriptive statistics to give context to participants' responses and the qualitative analysis (Section 3.2).

3.2 Results Overview

We recruited interview participants from our university community via posters, mailing lists, and word-of-mouth. At 27 participants, we reached saturation, where we were hearing little new from additional participants.

Two-thirds of participants were female. Participants' age ranged between 17 and 67, with a median age of 22. Most participants were either full- or part-time students and came from a range of programs including the humanities, sciences, and social sciences. None of the participants were studying computer science or computer security. The other participants worked in the university community in roles such as administrative assistant, librarian, and security guard. We deliberately recruited users without educational background or explicit work experience in computer security.

Participants reported their total number of accounts as between 9 and 51 accounts, with a median of 26 accounts. The bulk of most participants' accounts consisted of email addresses, university or work accounts, and social networking accounts. They reported using between 3 and 14 accounts in an average week, with a median of 11 accounts.

Participants reported having between 2 and 20 unique passwords, with a median of 5 passwords. All but one of the participants in the study (26 participants, 96%) reported reusing passwords between accounts. Of the participants who reported reusing passwords, most (23 participants, 88%) reported reusing more than one password, and 19 (73%) reported reusing passwords either "always" or "frequently."

The next set of questions addressed the coping strategies that users develop to keep track of passwords and accounts. We asked participants if they used any kind of password manager (including the browser-based managers), and 22 respondents (81%) said that they saved their passwords in some kind of password manager. All of these went on to clarify that they saved passwords in their browser or in the Apple Keychain. No one reported currently using dedicated password management software, although one participant said that they had previously used one.

Twenty-one participants (78%) reported writing down at least some of their passwords. Of these participants, most referred to the recorded passwords as a backup for memory and not a resource used at every login. Participants reported using both physical and digital media to store passwords, but specified that the recorded passwords were easily accessible from their regular computing context.

The final part of the interview asked participants about password changes and resets of forgotten passwords. Forty percent of participants reported having ever changed passwords of their own volition, and these participants remarked that they changed passwords rarely and only under special circumstances. All participants reported having changed their passwords to reset a forgotten password.

3.3 Grounded Theory Analysis

We chose not to fully transcribe our recordings. Instead, we made detailed notes about responses to the interview questions. These notes included quantitative question responses but also included additional details from participants' discussion of the topic. In places where our notes were not sufficiently detailed, we returned to the audio-recorded data for additional information. We referred to the audio recordings to transcribe exact quotes for use in this article.

For the qualitative analysis, we followed the Grounded Theory methodology of Strauss and Corbin [41]. This method involves several steps in the analysis process. First, recorded data are analyzed point by point and assigned descriptive codes in the process of *open coding*. Next, these codes are compiled, and the process of *axial coding* looks for relationships among the codes. In the process of axial coding, the researcher asks questions such as *why*, *where*, *how*, and *when* in an effort to uncover structure in the data. Finally, *selective coding* integrates the results of the open and axial coding and refines them into a theory.

3.3.1 Open Coding. We generated open codes by examining the noted responses from the interview data. We traversed the answers to each question, looking for recurring patterns and themes in the data. Each of these themes was denoted by a code.

Some of the codes emerged in relation to the question being asked in the interview. For example, we asked participants about whether they wrote their passwords down and how they stored and referred to recorded passwords. Several codes about password recording emerged from responses to that question. However, other codes emerged over the sequence of the discussion. Participants gradually revealed more about their password creation, organization, and categorization

Fig. 2. Rearranging the codes to look for patterns in the axial coding process.

techniques as we explored how they would handle password creation, how they would choose passwords for new accounts, and how they would keep track of new accounts.

One of our password recording codes was *records passwords as backup strategy*, and we used this code when a participant indicated that although they wrote at least some of their passwords down, they did not refer to these recorded passwords on a regular basis and instead appeared to use the recorded passwords as a backup. In the following quote, the participant describes how she used to write her passwords down as a fallback for memory when going on vacation:

> Not any more. I used to. [Why did you stop?] Because the only reason to write them down was if I was going on vacation for two weeks and I'd come back to work and I wouldn't remember my password [laughs]. So that was [garbled] but now I very rarely take vacation more than one week at a time and I can remember one week [laughs]. (P15)

This participant describes writing her work passwords down so that she would be able to remember them after a long delay. However, she does not need this technique in everyday use. She also explains how a change in her circumstances (shorter vacations) has affected her password coping strategies (coded as *change of habit*).

3.3.2 Axial Coding. Following open coding, we began the process of axial coding. In axial coding, we took the codes assigned in open coding and looked for patterns, connections, and relationships between those codes. Our eventual goal was to form a model or theory that described our data. To examine the codes, we tagged each code with a post-it note and arranged them on a table to look for connections (Figure 2).

We began the axial coding by collecting codes with a similar focus. Following this, we identified a temporal ordering and then assembled our groupings into larger categories following this order. These categories are described in the subsequent sections.

Choose Your Password: At some point, every user must create their passwords and how they do this is up to them. In our interviews, participants discussed a number of strategies that they employed when choosing passwords. Some participants included personal information in their passwords. Participants mentioned including the birthdays of loved ones, phone numbers, and personal information such as hobbies in their passwords:

> I'll try to usually think of some kind of hobby of mine, uhh, whether it would be something like hockey or a video game and a video game character, and I'll try to link it to that. Something that I usually think about quite a bit. (P24)

These strategies were often combined with affective strategies that included personally meaningful information in passwords. One participant told us that she had changed her passwords to state a personal goal, so that the password would be easy to recall but also so that she would be continually reminded of the goal:

> I read an article this, this, uhh, month, that said 'whatever your goal is, make that your password' [okay] and you can still follow their rules … but because you're going to be entering in your password so many times a day, make it your goal, and it can be anything, you know. (P15)

Another participant said that she included religious phrases such as "God is good" in her passwords, as a reminder of her beliefs and priorities.

A few participants mentioned an algorithmic strategy for creating passwords. They systematically combined pieces of information to create passwords with a consistent format. Participants described different pieces of information that were included in their passwords. One participant said she included a piece of information associated with the website, as well as a piece of personal information in each password. Participants also had a few standard symbols, numbers, or words that they recombined for variation in their passwords.

Reuse Your Password: Password creation always happens with a new account, but users almost always have other accounts as well. Most of our participants reused passwords across accounts. We were interested in how they chose to reuse passwords across accounts and how they matched passwords with accounts.

The participants in our study who reused passwords all built a personal model of reuse. Often, participants described categorizing their accounts and assigning passwords to categories. Participants described a number of different categorization strategies. Security was a common consideration that many people mentioned:

> Like I said, it depends on what the website actually is. If it requires a weak password according to me or a strong one, I'll choose it on that basis and probably alter a letter or two. (P25)

Participants assessed the security needs of the websites, and they referenced matters such as privacy and confidentiality without clarifying those terms. Many participants explained that they treat accounts differently if they store credit card information. We were unsure of how they assessed the security needs for non-financial personal information (such as on social networking websites).

It was clear in the interviews that although many people had several reused passwords, there was a primary password that was reused on most accounts. Participants referenced this password in a variety of ways, but the language used indicated the importance of this password. One participant called it her "go-to password" and told us that she relied on it because she trusted the person who had chosen it for her. Several participants referred to a certain password as being "familiar" or "easy." Many participants remarked that they had many passwords that were variations on a single password, and it appeared that these were often variations on this most-used password:

> [How many unique passwords do you have?] Eight? But it's always, like, you know, adding a one at the end when I forget. [So some of them are slight variations?] Yeah, yeah. (P9)

Commit Your Password: After assigning a password to an account, the user must be able to keep track of this password. In our study, participants described a variety of coping strategies that they used to remember (in the active sense – store) their passwords.

The majority of participants told us that they wrote at least some of their passwords down. Some participants described strategies where they recorded all of their passwords, and others told us that it was a strategy that they used only in special cases. Most participants said that they wrote their passwords down to prevent forgetting them, but others wrote their passwords down as part of a larger strategy. One participant told us that she records her passwords in a spreadsheet for her husband to access in case of emergency. She later implied that she sometimes consults the spreadsheet for herself, but this is not the primary reason for keeping it:

> [Do you ever write your passwords down?] Only maybe a couple of banking ones, they're the only ones, my banking, so if I die my husband can find them. (P5)

Most participants appeared to view their password recording as a backup strategy rather than a constant resource. Some regarded it as an interim strategy. One participant told us that she wrote passwords down only until she had memorized them and that she also used a rehearsal strategy to help her memorize her passwords:

> If it's new, I'll write it down for the first couple of times, but if it's new, I'll try to remember it, try to memorize it. I'll log in a bunch of times until I've memorized it. (P11)

A number of participants described special cases where they would write passwords down. These special cases included assigned passwords, websites without any backup mechanisms (such as online password resets), and websites where the use of cookies is disabled. Other participants told us that they recorded hints or clues to their passwords: "I put something to remind me what the password was" (P13).

An important consideration in the safety of recording passwords is how they are stored. Participants in our study described a variety of storage strategies for recorded passwords. Some participants wrote down their passwords on physical media, such as post-it notes or journals. Others stored their passwords digitally, in dedicated lists (Excel spreadsheets, or Word documents), emails to themselves, online notebooks (such as Evernote), or password managers.

The accessibility of recorded passwords was a key issue. Participants who chose to store their passwords digitally often mentioned concerns about having the password list when it was needed. One participant emphasized the need for accessibility when he described using services that synced across devices to store passwords:

> [Do you ever write your passwords down?] On my phone, sometimes. …Usually you would either keep it in, like, Google Keep or iCloud or messenger or Evernote. In my case, Evernote. I use a lot of Evernote, so … Anything that is really sync-able to multiple devices that way it is easier for me to store info. (P16)

Although a single sign-on option ("Connect using Facebook," see Figure 3) was prominently displayed on the password creation prop card, only two participants commented on it. One participant told us she would use the option when it was available because she had a hard time remembering even her reused passwords. However, another participant said she would not use it, because she did not want any extra information cluttering her Facebook page. It is difficult to know why other participants did not mention any kind of single sign-on, since the cue was equally visible to all participants. Our interview script did not prompt them to specifically look at the Facebook button,

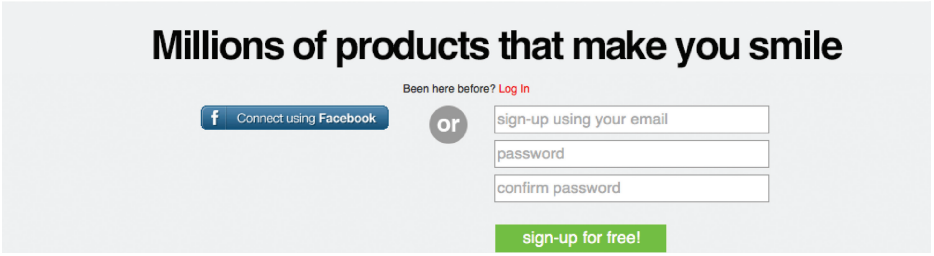

Fig. 3. A detail of one of the websites used as a prop in our interviews.

but they were told to imagine they were on that page. Possibly, this indicates that most users do not understand how single sign-on services can be used as an alternative to reusing passwords.

Forget Your Password: After a user has memorized his or her password, there is always the chance that he or she may forget it. Users have many passwords, and it is clear that handling forgotten passwords is a large part of the password management task.

Several participants described situations where they could not remember their passwords at login and told us their first action would be to try and guess their password. Some participants described a kind of targeted dictionary attack on themselves, where they would guess all of their reused passwords:

> Sometimes, I do forget, but I try everything else [all of the passwords]. (P17)

Other participants described guessing strategies where they attempted to recreate their motivation for being on the site (for example, the item they were buying when they created a shopping account) or the password they would have been likely to pick in the time period they created the account. Still others said they would try to recreate algorithms for password creation or look at the password policy to make a better guess at their own password.

The other fallback strategy that participants described was the password reset mechanism. In this, we include both personal verification questions and email resets. Almost all participants told us that they had reset forgotten passwords, and it appears that many users do this on a regular basis. Some users seemed fine with this as a strategy, but others raised objections. One participant told us that she had begun writing her passwords down when she realized she was resetting her passwords too often. Another participant remarked that she had not considered how often she reset her passwords until the interview, but that it was a major part of her password coping strategy:

> It's funny, I never really thought about it, but I guess I do that a fair amount. (P19)

Live with Your Passwords: Passwords and accounts can last a long time: once passwords have been created and linked to accounts, all users must begin the long process of living and coping with their passwords.

A number of participants in our study commented on the difficulty of managing and remembering passwords. One participant referred to passwords as agonizing:

> Then what do I do? Ohhh, my gawd. Then I agonize for a few minutes. (P13)

Another participant seemed resigned to reusing passwords:

> [Do you ever reuse passwords?] Oh yeah! [laughs] (P9)

Participants also referred to fears of doing the wrong thing and uncertainty about the outcomes of password decisions.

As time progresses, a user may change his or her behaviour in some way. In our study, a number of participants described changes in behaviour that had occurred for a variety of reasons. Some users described stopping or starting using tools. One participant told us that she no longer saved passwords in the browser because she had heard that this behaviour could be dangerous.

One reason to change an existing password is in the case of a security breach. A number of participants in our study described situations where they had changed account passwords after suspecting that an account was not secure. Examples of breached accounts included email and PayPal accounts. As participants described their security breaches, it emerged that they were often unsure about whether they had been attacked and sometimes had to made decisions without really knowing what had happened:

> At least, I think that I've been hacked. [What kind of clues, what would be a kind of signal to you? Has it ever happened to you?] It has, because my friends told me they got these really strange emails, from my email, supposedly sent from me, that were obviously ads for something or other and they were like "Hey, this doesn't sound like you." (P19)

3.3.3 Selective Coding. The last coding step in Grounded Theory is selective coding, where the researchers attempt to identify a unifying *core code* that describes the underlying phenomenon in the observed and interpreted behaviour.

As we analyzed the data, a central theme about rationing and budgeting began to emerge. In all phases, our participants described ways in which they stretched thin resources: memory, attention, creativity, and security knowledge. Similarly to the way in which we ration and conserve time, energy, food, and money, participants were handling password management by devoting appropriate resources to accounts of great importance, devoting less energy to other accounts and generalizing their approach to similar accounts to save effort. We do not suggest that this budget is necessarily fixed but rather that users' efforts, attention and memory are limited and users must be thoughtful in their commitments. In their work on organizational security, Beautement et al. [7] suggest that organizations need to budget for the costs (both time and money) of organizational compliance. Our suggestion about rationing differs in that we identify that individual users are budgeting their own time and effort. We are not suggesting this arises because of a lack of willingness to comply but rather from a paucity of cognitive resources.

In the following sections, we systematically examine how rationing plays a role in each of the themes of axial coding.

Choose Your Password: When choosing their passwords, participants rationed their efforts in a variety of ways. For participants with formulaic or algorithmic strategies, part of their investment was in memorizing their personalized strategy. By remembering that their strategy was to include a word related to the website, they reduced the amount of effort that it takes to choose a password on a new website.

We asked participants what they would do when creating an account if their password was rejected on the grounds of insufficient complexity (for example, lacking a symbol). Most participants reported that their strategy in this situation was to append a symbol to the password. Most participants referenced "their" symbol and told us that they had a habitual symbol that they used in this situation. This coping strategy implies a way of rationing effort across situations that cannot be predicted. If participants knew their password would need a symbol, then they would have begun with a symbol. But since they are unable to see the password policy, they have developed sensible coping strategies that conserve memory and effort in these situations.

Reuse Your Password: One main way in which users ration their efforts is in not choosing a new password for every account. Reusing passwords allows users to conserve energy across their large number of accounts.

As participants discussed how they would create a password for a new account on an online shopping website, many digressed into a discussion about accounts that do not matter to them. One participant told us that she had a password that she reused on accounts where she would not care if she was hacked. Another participant referenced having a password that she would not mind sharing with others. Whether or not these participants actually would not care if others had access to their account, their behaviour shows that they are rationing the effort they put into these accounts by the amount of concern they merit.

An important aspect of rationing is that those who need more should get more, and we found evidence that users were applying this principle in their password management strategies. Many participants referenced special habits for their online banking: Participants told us that they did not reuse their banking passwords, that they would not log into their bank on a shared computer, and that they would not enable cookies or save their banking login in the password manager. All of these behaviours indicate that users are willing to ration more effort into accounts with higher perceived importance.

Commit Your Password: Memorizing passwords is one of the most difficult parts of the password management task for users. Passwords must be maintained over long periods of time, with sporadic and unforeseeable usage patterns. Participants in our study described using a combination of techniques to keep track of their passwords. Some participants were heavily invested in one strategy, but most participants appeared to know a few of their passwords, to have some of them written down and to have some of them stored in a password manager. This strategy seems to ration effort across time and place—when at home, the browser saves the passwords for almost all of their accounts, or they might have easy access to the recorded passwords. When elsewhere, they cope by remembering their passwords or by carrying some of the passwords with them. It appeared that some participants were sacrificing convenience for security in these situations, which indicated another aspect of rationing in their coping strategies.

Forget Your Password: All of the participants in our study told us that they have reset passwords when they are forgotten. Participants clearly regarded this as being separate from a change of password, which seems to indicate that forgotten passwords are seen as part of the landscape of password management. Users expect to have to handle a loss of memory or a failure of a coping strategy. It appears that the password reset mechanism allows users some flexibility in their rationing strategy. In situations where a password reset was not available, participants described allocating extra effort to the situation, often to ensure that the password was recorded.

Live with Your Password: Throughout the interviews, we heard a number of remarks on the difficulty of password management. Although participants were resigned to the realities of passwords, passwords still present difficulties. Finding and implementing coping strategies for the difficulties of passwords involved effort and unpleasantness. Similarly, rationing itself is a difficult task. The decisions about how to allot time, energy, and effort are not always obvious to users. Users referred to missing information that would have made it easier to cope: unseen password policies, misunderstood security requirements, and invisible security breaches.

3.3.4 The Password Life Cycle. In the final step of Grounded Theory, we look back at the identified codes, patterns, and relationships to form them into a theory.

Our theory is that there is a password life cycle—a progression of stages through which every password passes. Passwords are created, assigned to an account, recorded or memorized, lived with, and then potentially forgotten. Old passwords are then reused or adapted in the creation of new passwords, and the cycle continues.

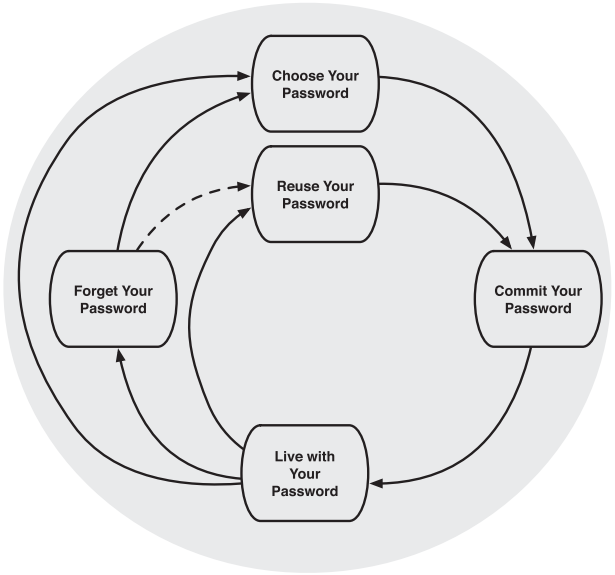

Fig. 4. The password life cycle.

Figure 4 illustrates the stages of the password cycle. The cycle begins when the user needs to create a password for a new account. Theoretically, a user might begin with no passwords at all and have to fabricate one from scratch, but they may also have existing strategies and password phrases that they will integrate into a new password. This password must next be committed, either memorized or recorded, so that it can be later used for login. Assuming that the commitment process is successful, the user then lives with his or her password. They login and access their accounts successfully. If they successfully remember their password, and it is appropriate for reuse, they can then reuse that password. If the password must be changed (because it is forgotten, because someone else has learned it, or because of enforced password change policies), then they must return to password creation.

The cyclic nature of the life cycle reflects how prior events affect users' password management strategies in an ongoing way. Changes propagate slowly through coping strategies, and users rarely completely abandon a password or a memorization strategy, instead harvesting the parts of the strategy that worked for them and reusing those techniques on other accounts. Users reuse passwords (or parts of passwords) on multiple accounts and in different ways over multiple iterations of the life cycle. Because of the investment inherent in creating a password management strategy (which involves choosing a password, finding a commitment method, living with that password, and coping with failures in that strategy), it is impractical for users to start afresh with every new account and instead cyclically revisit previous passwords and habits as they cope with account after account.

Rationing is present at every step of the password life cycle. Users ration effort in creating new passwords, they reuse passwords to put more protection on the most valued accounts, they reduce the effort of memorization by saving passwords in managers or by writing them down, and they strategically budget the attention they pay to passwords on existing accounts. Users save resources from inconsequential accounts so that they can devote them to more important accounts. Allotting time, attention, and energy to different accounts forms the backbone of users' coping strategies. As with other forms of rationing, users may scrimp on effort for some accounts to save it for others.

Rationing contributes to the cycle of password reuse. As effort is reduced from some accounts, it is saved for new ones. Reused passwords are handed down (in whole or in part) from existing accounts, saving the user the time and energy of creating and memorizing a new password and leveraging the effort previously invested into passwords. This is sensible, rational behaviour on the part of users that allows them to cope with the impossible demands of passwords. Although these coping strategies are considered responses to the demands made of users, security problems (such as password breaches) still remain.

3.4 Summary

Users create successful strategies to cope with the impossible demands of passwords. They reuse passwords to conserve the effort of creating and remembering new ones and save resources for the accounts that they deem most worthwhile. These coping strategies are rational and make sensible tradeoffs based on the availability of cognitive resources and the demands of different accounts. However, users encounter problems related to both usability (password forgetting or loss) and security (account compromises), indicating that there is room for improvement in their coping strategies.

4 STUDY 2: HOW DO EXPERTS MANAGE PASSWORDS?

In our second study, we conducted a series of interviews with researchers and practitioners in computer security, asking them about their password management behaviour. The goal of our interviews was to better understand the practices of expert users and to see how they address the demands of creating and managing large numbers of passwords. Do experts rely on similar coping strategies as non-experts? What kind of tools and techniques do they use? What differentiates experts from non-experts? We hoped to find insight from the practices and coping strategies of experts to help us form recommendations for non-experts.

The purpose of this study was to add a new perspective to the interview data and analysis conducted in Study 1 by interviewing a different user group. In qualitative analysis, *triangulation* is the process of adding additional information and perspective to the analysis. The purpose is not to confirm the findings but to add additional viewpoints. Our goal was to understand whether (and how) the life cycle model appeared in this different population and whether any insight could be gained from how experts cope with passwords to provide assistance for non-experts.

4.1 Method

To investigate how computer security experts manage their passwords, we conducted another series of semi-structured interviews using the same interview script as in the first study. Once again, the interviews were conducted by the researcher, who asked questions and recorded responses, and the interviews were audio recorded to facilitate further note-taking. We encouraged participants to elaborate on incomplete answers and to pursue alternative discussion paths that revealed the details and complexity of their password management strategies. The study was approved by the Carleton University Research Ethics Board and the ETH Zürich Ethikkommission.

We interviewed 15 expert users, recruited using a snowball sampling technique [22] from the community of industry security practitioners and from among the information security research groups at ETH Zürich. Reflecting the gender distribution of the security community, the majority of our participants were male (13 participants). Participants ranged in age from 24 to 35, with a median age of 29. All participants except two had a graduate degree in computer security and all were employed as researchers, graduate students, or practitioners in information security.

In recruiting for the study, we took a conservative approach to defining expertise. We deliberately recruited participants whose expertise was based on formal educational credentials in

computer security and who were actively working in the field. While we did not measure expertise, we took real-world credentials (rather than self-declarations) as an indication of expertise. Different participants' expertise may not have been exactly equivalent, but they were all well versed in computer security topics, of which authentication is a basic requirement.

4.1.1 Triangulating the Password Life Cycle. We began the expert interviews with the expectation that experts' password management strategies would significantly deviate from what was described by the non-experts. Contrary to our expectations, our first observation was about the similarity of described behaviour. Like the non-experts, experts described difficulties creating passwords, systematic password reuse (and variations on reuse), use of a "go-to" password, and problems remembering passwords and described the difficulties of living with passwords. They also described the limited resources available to them and the decisions to allot effort differently to different accounts, fitting into our core code of *rationing* from the life cycle analysis.

Following the process of open coding, we decided that the more interesting question about the experts data was not to examine how it resembled the non-experts but to examine how it differed. Thus, we chose not to follow the same Grounded Theory analysis as in the first study and instead conducted a thematic analysis of our qualitative data, using methodology described by Braun and Clarke [9]. We chose thematic analysis for its flexibility and because it allowed us to explore the depth of our data and better understand the commonalities of participants' discussion and responses. Since the coding process was very similar to that in the first study, we simply present the categorized findings here.

As in the first interview study, we had two datasets: a quantitative dataset of participants' specific responses to yes/no and quantitative questions and a qualitative dataset of participants' explanations and detailed responses.

4.2 Results Overview

The expert participants in this study had a median of 63 accounts, and reported using a median of 10 accounts in an average week. They reported wide ranging numbers of unique passwords, from 4 to 200, with a median of 25.

We were very clear that participants should not share their passwords with us, and experts were understandably private about their exact password creation strategies. Although participants did not discuss the exact components of their passwords, most participants said that their passwords were rarely rejected for failing to comply with password policies, indicating that these experts were including special characters, digits, and capital letters in their passwords.

Although password reuse is a technique often criticized by security experts, the majority of our participants (80%) said that they reused passwords on at least some of their accounts. Of those participants who reported reusing passwords, all said they reuse multiple passwords. The median number of reused passwords was three. Most participants described a careful strategy for reuse, and often said they did not reuse all of their passwords, but that they had one or two passwords that they consistently reused for "throwaway" accounts. Participants mentioned reusing specific passwords for specific purposes, such as single-use websites or seldom-visited websites.

When discussing the kind of password that they reused, participants were clear that they had "their" password, often naming it (e.g., "my bootstrap password" – E14). Multiple participants referenced having had their password since they began using computers and one mentioned having had their password since high school.

We asked participants about how they stored passwords, and most (80%) reported storing their passwords in a computer program. Of these, half reported using a dedicated password manager, and half reported storing their passwords in a web browser. Of the participants, 60% told us that

they wrote their passwords down. All but one of these specified that writing their passwords down was something they did rarely and only when unavoidable (e.g., in the case of an assigned password that they could not remember); the remaining participant treated his list as a kind of password manager but also said one of the purposes of his list was to give to family members in case of emergency. Several participants said that they relied on their password manager to generate passwords for accounts, but others said that they did not use this functionality (in spite of using a password manager to save passwords). Some participants described only generating random passwords for certain accounts, and most often said that they used this functionality for high-importance accounts.

Slightly less than half of the participants (47%) reported that they will enter their passwords on computers belonging to friends or family members, but most qualified the statement by mentioning that they will only log into certain accounts on other people's computers. Those who said that they would not enter their passwords on systems not managed by them said that this was a deliberate and strict policy.

4.3 Thematic Analysis

We began our thematic analysis with the process of open coding and we traversed the notes from our interviews, assigning codes to the data. We identified a total of 30 codes, some of which were present in the earlier analysis and some of which were new.

Following open coding, we began the process of identifying themes and relationships in the data. We identified four broad themes in our data, each of which addresses some aspect of our research question: How do experts manage passwords?

4.3.1 Expert Awareness. During the interviews, it was clear that a key strategy for expert participants was to have consistent and pre-planned strategies. Experts were able to speak knowledgeably and fluently about their password management and security strategies. They were familiar with what they do to address security and often anticipated subsequent questions in the interview. While this familiarity is no doubt due to the fact that these participants spend large amounts of their lives considering security, it also highlighted the *a priori* nature of the expert approach. These participants referenced specific policies and were emphatic about avoiding certain situations.

Experts were specific about how they create and adapt passwords, and when asked the same question in different contexts, they often showed confusion about why the question was being asked again. Our interview asked about password creation when creating a new account vs. resetting a forgotten password, and at the second question, many participants gave us answers such as:

> [If you do have to reset a password because you don't remember it, how do you pick the new password?] Uh, I mean [it] is the same technique as I used before. (E02)

Experts also showed awareness of specific threats in the interviews. When we asked about password changes, several experts referenced having changed their passwords in response to Heartbleed, a security bug in the OpenSSL library that necessitated widespread password changes:

> Well, there's, there's been a couple of incidents like, uhh, my laptop got stolen at one point, or… Or maybe you hear, like, a serious vulnerability like Heartbleed, and that's when you think that, that this might be a time to change passwords. (E07)

Planning for security can be made difficult by the myriad other pressures and unexpected situations that can arise, and experts did mention these situations that forced them to deviate from their preferred strategies. Among the situations described in the interviews were the pressures of

friends and family, as well as unforeseen circumstances where information needed to be retrieved. The social and contextual pressures that affect everyone also affect computer security experts:

> I can be as paranoid as I want, but you know, in the real world I have a family and stuff, so sometimes you have to make compromises. (E15)

4.3.2 Combining Strategies to Remember Passwords. Participants described a number of strategies for managing their passwords and accounts, and unexpectedly, many experts described using more than one technique, depending on the account.

Almost half of the participants said that they wrote some passwords down, and all of these described it as a kind of backup strategy. One participant said he wrote down passwords that were difficult or impossible to change. Another said that when he was issued assigned passwords, he often kept the piece of paper that came with the password (e.g., a letter with a PIN sent by the bank). One participant said that he wrote down most of his passwords, but was explicit about how his strategy was intended as a backup strategy for infrequently-used accounts:

> I just keep them written down just in case, and there are those more throwaway accounts that I use once every … a few times a year, but I need then to check. (E04)

Twelve participants described using some kind of password manager to save passwords. Six participants told us they used dedicated password managers, and 11 participants reported saving passwords in the web browser or in applications. Most participants mentioned using more than one tool, and even users of dedicated password managers reported using them alongside the browser-based managers.

Several participants described using a combination of strategies. In particular, multiple participants mentioned using password reuse in combination with password managers. One participant said that he used a password manager to randomly generate and remember passwords for important accounts, but that he opted to reuse passwords instead of storing them in the password manager for insignificant accounts:

> I don't store everything in a password manager. [Why not?] Because I, I dunno, because that's kind of incon… It's just another layer of inconvenience to use a password manager, and I, for me personally, it's not worth the investment to store it there. And it also kind of clogs my database, I guess, if I would store it in there, the password manager. (E01)

Although this participant uses a manager, he weighs the inconvenience of the password manager against the significance of the account before deciding if he will use the manager for that account.

4.3.3 A Personal Assessment of Risk. Experts often explicitly mentioned the personal assessment of risk that played a role in their password management and creation strategies. One of the problems of computer security is that it can be difficult to know how well an account is protected and to what level an account needs protection. Even with the additional experience and knowledge that accompanies expertise, it is hard to know exactly how specific decisions and choices will affect the protection of an account. In the following quote, the participant corrects himself to clarify that his classification of his two passwords as secure is based on his own judgment:

> I have two passwords that are, um, that I *consider* to be more secure, and that I use for only few things, but yeah, I consider more valuable. (E04)

This idea of personal assessments of security came up repeatedly in the interviews, often in the discussion of a categorization strategy for accounts. Participants remarked on a number of

categorization factors, including money/financial information, service-based categorization, or simply "importance." These strategies were often vaguely defined, and experts sometimes acknowledged their own inconsistency:

> I actually buy train tickets with this [password], but, yeah, I am contradicting myself because buying a train ticket involves money but I don't really care! (E11)

Experts were clear in the interviews that objective assessments of security are difficult to make, and almost every description of a password management strategy mentioned this in some way. Experts did not express hesitation or concern about these decisions, but they were quick to clarify that many of their security assessments were particular to them. Having the awareness and ability to make these decisions quickly and relatively accurately is a hallmark of expert password management.

4.3.4 Usability Problems. Even though they were knowledgeable about password best practices, our participants still described difficulty and frustration with password management. One participant described assigned random passwords as "ridiculous string[s] of horror" (E03). Participants described a number of ways in which they anticipated and experienced usability problems with passwords. Several participants said that they did not expect to remember passwords that were modified to comply with unusual password policies, and one participant described problems remembering the usernames associated with passwords.

The usability problems of passwords also lead experts to make mistakes: Experts mentioned a number of practices with obvious security vulnerabilities. Since experts are presumably aware of these weaknesses, it is telling that they have chosen to trade off security for usability in certain situations. Two participants said that they sometimes created passwords using dictionary words from their non-English mother tongue. Dictionary words in any language are easy for an attacker to guess:

> I sometimes do pick words from my native language because they almost look like a garbled set of characters in English, and then it's highly unlikely that somebody gets it. (E10)

Another insecure practice mentioned by experts was guessing at their passwords. If an attacker is collecting password entries, then guessing multiple passwords can quickly leak many passwords to an attacker. More than one participant referenced this technique, though most did clarify that they would only turn to it for low-value accounts:

> Since those belong mostly to throwaway accounts, I will just try another variation or try another one of my standard set of passwords. (E01)

4.4 Rationing and the Life Cycle

In the interviews and coding process, we found evidence that the experts' password management techniques fit into the life cycle model. Experts described different strategies for creating passwords and described reusing passwords (sometimes with small variations) for long periods of time. They described graduating passwords from important accounts to less important accounts, and the process of committing passwords (whether through a password manager, writing it down, or to memory). They described the difficulties of living with passwords and the hassles of forgetting or losing track of passwords.

It was also clear that experts were rationing their efforts across different accounts. They adopted consistent strategies for password creation, reused passwords strategically to save effort from

undeserving accounts, and invested additional energy in important accounts by using a password manager or other higher-security strategy. They also described situations (such as Heartbleed) where devoting additional effort to activities such as password changes became more worthwhile than in everyday circumstances.

Apart from educational credentials and area of work, the main difference between the experts and non-experts was that the non-experts almost never discussed security problems. They brought up situations where global vulnerabilities affected them, but none of them related scenarios when they had experienced a personal breach (such as email sending spam, or the assumption that a friend had access to an account). Although our interviews did not measure security outcomes, experts did not seem to be experiencing the level of difficulty, shame, or guilt around password management that was exhibited by the non-experts.

4.5 Distinguishing Experts

Defining expertise is problematic, but it is usually agreed that an expert is someone with high knowledge in a certain domain and who is successful in that domain [17]. For example, an expert in chess is someone who is deeply familiar with the rules and strategy of the game and is able to use this knowledge to win many of their games. However, the notion of success is less clear in personal practice with passwords. How exactly can it be shown that someone is more successful at managing their passwords than another person? How can we know that a lack of security breaches is due to good management and not due to luck?

In "ill-structured problems" [37] such as computer security, Endsley [16] argues that expertise comes from skilled decision making, which is enabled by *situation awareness*. Situation awareness is

> the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future. [15, p. 97]

Along with specialized skills and high knowledge in a domain, strong situation awareness contributes to expertise.

Neither we, nor the experts themselves, can be completely certain that they are avoiding attacks. However, their detailed understanding of computer security, coupled with their general lack of description of personal security problems in the interviews, seems to suggest that their password management strategies are successful. We suggest that this knowledge might be regarded as a form of situation awareness.

Experts with high situation awareness have learned knowledge and skills, schemas for prototypical situations, mental models of the domain, and automatic processes in the domain [16]. In our interviews, experts demonstrated all of these characteristics. They had high knowledge of the security domain and awareness of specific threats. They recognized the kind of password-related scenarios they had encountered in the past and remembered their behaviour in those situations. They had mental models of threats and defences for those threats, as well as for which accounts were susceptible to which threats. Finally, the experts in our study had clear and automatic processes for how to create, remember, and reuse passwords in prototypical situations.

4.6 Summary

Experts lean on the same coping techniques as non-experts. They reuse passwords, write them down, and create weak passwords for insignificant accounts, but they also carefully consider whether these coping strategies are appropriate, and substitute more secure habits when needed.

Similarly to non-experts, experts have limited resources and must ration their efforts, but their increased situation awareness gives them greater success in managing their passwords.

5 STUDY 3: IS THE LIFE CYCLE THEORY GENERALIZEABLE?

As we emphasized in Study 1 (Section 3), the work on the password life cycle was theory-building, not theory-validating. Following the development of the life cycle theory and our investigation into how it was expressed in the interviews with expert users, we grew interested in how the model would hold up in a broader population.

Our Grounded Theory analysis showed that individual users use passwords in a cyclical method, first creating passwords and then committing those passwords to memory until they are compromised, forgotten, or out of date, at which point a new password is then selected, reused, or adapted from another password. Users ration their effort into maintaining and managing passwords, devoting additional effort to important passwords and accounts, and saving attention from accounts that need it less.

The life cycle theory (Section 3) was developed from an in-person sample of users from the Carleton University community in Ottawa, Canada. We reached saturation and stopped interviewing after 27 participants when we realized we were hearing little new in each interview. The findings were supported in the expert interviews (Section 4), which were recruited from security researchers in Zürich, Switzerland, but an open question remained about whether the theory is applicable to larger populations.

To investigate how the password life cycle model generalizes in a more diverse population, we conducted a survey-based study. The survey asked a wide variety of questions about exactly what users do to cope with the demands of passwords and how well users feel they are handling those demands. By better understanding how the behaviours and themes that we identified in the interviews occur in a larger population, we can better design ways to either safely support these behaviours or to discourage and replace them with safer behaviours.

5.1 Method

We designed a survey instrument based on the findings of the life cycle. We chose to use a survey for the research, because it did not require the presence of an interviewer and could thus be easily and efficiently distributed to a large group of respondents.

We developed our survey based on the phases of the password life cycle. The survey had seven question groups, each focusing on a different aspect of password management. These groups included sections on choosing passwords, reusing passwords, saving passwords, changing passwords, and perceptions of password security. We also included a group with some basic questions about password and account use, as well as a demographics section. The questionnaire was approved by the Carleton University Research Ethics Board.

The section on password use echoed the questions asked in the life cycle interviews and was included to give a comprehensive picture of respondents' online habits. It also provided a means of comparing the online sample to the two in-person samples, non-experts (Section 3) and experts (Section 4). The demographics questions were also similar to those included in the interviews and were again included to give a better understanding of the sample.

The main question groups were each based on a theme identified in the axial coding procedure during the Grounded Theory analysis of the non-expert data, though they were not identified as such to the respondents. In developing each group, we carefully combed the results of the qualitative analysis and developed questions based on the behaviour revealed in the interviews. For example, in the section on choosing passwords, we asked respondents to rate how frequently they included different types of personal information, including birthdays, names, and addresses, in

their passwords. Because we did not see evidence in the qualitative data that users were explicitly aware of their own rationing and the cycles of their own passwords, we refrained from asking explicit questions about their use of these techniques. Rather, we attempted to validate how the associated behaviours of the password life cycle and rationing showed up in the behaviour of a wider sample.

The survey used a variety of question types, including Likert scales, multiple-choice questions (i.e., "choose all that apply . . . "), yes/no questions, numeric fill-ins, and a few text fill-ins. For many questions, we asked respondents to rate how frequently they engaged in a specific behaviour rather than asking a yes/no question. This was intended to capture the full spectrum of behaviour and some of the diffidence revealed in the interviews. In the interviews, respondents frequently told us that they did something only occasionally and were unwilling to strongly commit to a statement of the format "I do . . . ".

In line with best practice for survey design, we designed our survey to minimize the effects of response bias. For questions with multiple parts, we randomized the order of presentation for subquestions. This was done to prevent an effect from respondents who focused more on the early questions. We also reversed the wording on some questions so that respondents would not be tempted to simply fill in the same response all the way down a question. Finally, we included a few duplicate questions that asked the same questions in different parts of the survey and used these to evaluate whether respondents were reading the survey carefully.

We conducted the survey on Amazon's Mechanical Turk [5], an online micro-working platform that allows access to participants from around the world. We chose Mechanical Turk to give us easy access to a large and more diverse survey sample. Our survey was implemented using LimeSurvey [34], an open source survey platform that allowed us to collect and store data only on our secure servers. Participants were paid $1.00 USD for their participation.

5.1.1 Survey Participants. We collected 348 complete responses to the survey (three questionnaires from duplicate respondents were removed). The only restriction on study participation was age; our ethics committee required that we restrict participation to those aged 18 or older. We did not restrict participation in any other way, based on the idea that we were interested in diverse responses.

Of the respondents, 60% were male and 38% were female (the remaining 2% did not state their gender). The survey sample was quite young (90% of participants reported being 45 or younger). Of participants' IP addresses, 90% were in the United States, 7% were in India, and the remaining participants were from countries scattered across the globe. The majority of participants (95%) reported English as their mother tongue, and the next most common first language was Tamil (2%). Respondents' educational achievement was high, as 45% reported having a university degree (undergraduate or graduate) and 23% had a college or professional qualification. Respondents reported a diverse list of professions, and only 4% reported that they were students. We asked participants to self-report their computer security expertise, and 30% of respondents reported themselves as knowledgeable or expert in computer security.

5.2 Results

We present the survey results organized by question group.

5.2.1 Password Use. The first question group asked respondents about how many accounts and passwords they had. The questions in this section were very similar to those asked in the interviews and were intended to provide a basis for comparison. Table 1 shows descriptive statistics for the number of reported accounts, accounts used every week, unique passwords, and reused

Table 1. Password Use Statistics for Studies 1, 2, and 3.

	Study 1 (Non-experts)		Study 2 (Experts)		Study 3 (MTurk)	
	Mean	Median	Mean	Median	Mean	Median
Number of accounts	27.2	26.0	67.5	63.0	25.2	21.0
Accounts used in a week	11.0	11.0	13.2	10.0	16.2	13.0
Unique Passwords	6.2	5.0	61.2	25.0	8.5	5.0
Reused Passwords	2.9	3.0	3.1	3.0	3.2	3.0

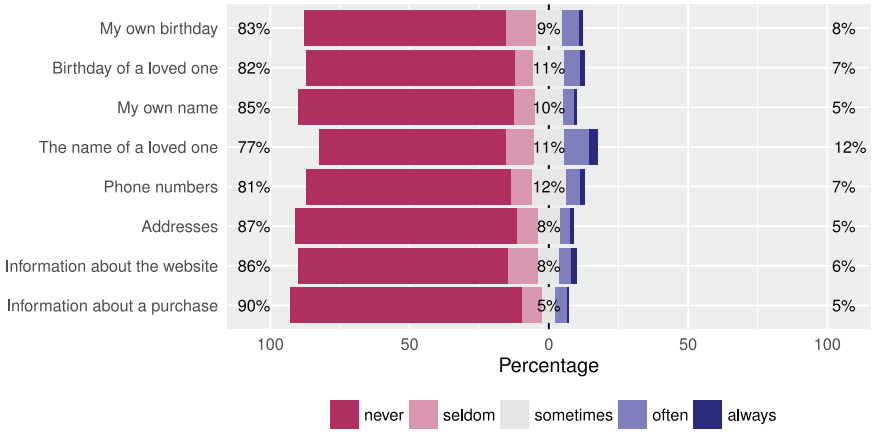

Fig. 5. Responses to rating scale questions about how frequently respondents include various types of personal information in their passwords.

passwords. These statistics are similar to what was reported in the earlier interviews with non-experts (Section 3.2).

5.2.2 Choosing Passwords. Figure 5 shows the distribution of frequencies with which respondents reported using personal information in passwords. Of respondents, 41% indicated that they often or always include *at least one* of these types of personal information in their passwords. To comply with password policy expectations, almost half of all respondents said that they "often" or "always" reach for a particular digit (47%), capitalize a particular letter (46%), or use a particular symbol (38%).

We also asked respondents about whether their passwords corresponded to external factors such as time periods, usernames, or password policies. Almost half of respondents said that they had passwords matching a particular password policy (49%). More than a third of respondents told us that they had a systematic way of combining information to create passwords (39%). Of these respondents, the most commonly used elements were a standard word and a standard number/digit.

5.2.3 Password Reuse. Three-quarters (75%) of respondents in our survey reported reusing passwords, and almost all of those (91%) said they did so because reused passwords are easier to remember. Other reasons for reusing passwords were convenience (67%) and speed (53%).

With such a high rate of password reuse, it is unsurprising that respondents reported reusing passwords on many similar kinds of accounts. Figure 6 shows the reported frequency distribution for different kinds of reuse. In all situations, most respondents reported reusing passwords "often" or "always." We also asked respondents who reported that they reuse passwords about the accounts

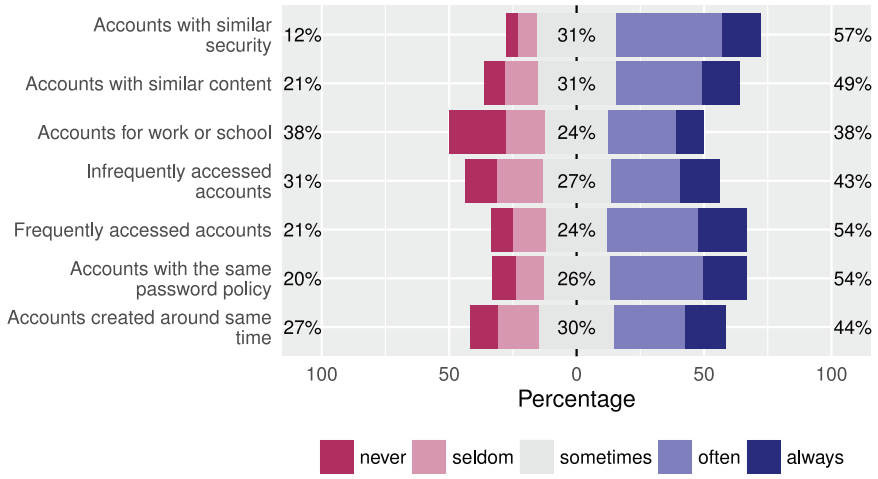

Fig. 6. Responses to rating scale questions asking about how respondents reuse passwords.

on which they avoid reusing passwords. The most common accounts where participants avoided password reuse were online banking websites (62%) and websites that store credit card information (43%).

In the interviews, many respondents referred to a particular password when discussing reuse. About two-thirds (60%) of survey respondents said they had a "go-to" or primary password. Of those, most said that they created variations of this password to use on different accounts (81%) and that they had a standard way of creating these variations (71%).

5.2.4 Saving Passwords. Users who have not memorized all of their passwords must use some means of saving those passwords. In this section of the survey, we asked respondents about their use of password managers (browser-based and dedicated), as well as their password recording strategies.

The majority of respondents (61%) reported that they "never" or "seldom" wrote their passwords down. Respondents were most likely to say that they recorded infrequently used and high-importance passwords (48%). Half of respondents (51%) reported that they wrote their passwords down in case they needed them, and 43% said that they did not usually refer to their recorded passwords.

Only 17% of respondents reported saving their passwords in a dedicated password manager, but 50% reported saving their passwords in a web browser. Of the respondents who reported saving passwords in the browser, respondents were most likely to say they did not save banking passwords (61%) or passwords for accounts that saved credit card information (39%).

Of the respondents who reported using a dedicated password manager, most reported using it for some combination of convenience and security. Most users took advantage of all password manager features: users reported saving both high- (72%) and low-security (76%) passwords in the manager, and slightly fewer (58%) reported using the manager to generate passwords. Of the respondents who said they did not use a password manager, the most common stated reasons were a lack of trust (44%), no need for one (36%), and an unwillingness to set one up (28%).[1]

[1]Respondents were allowed to pick more than one choice, so percentages do not sum to 100.

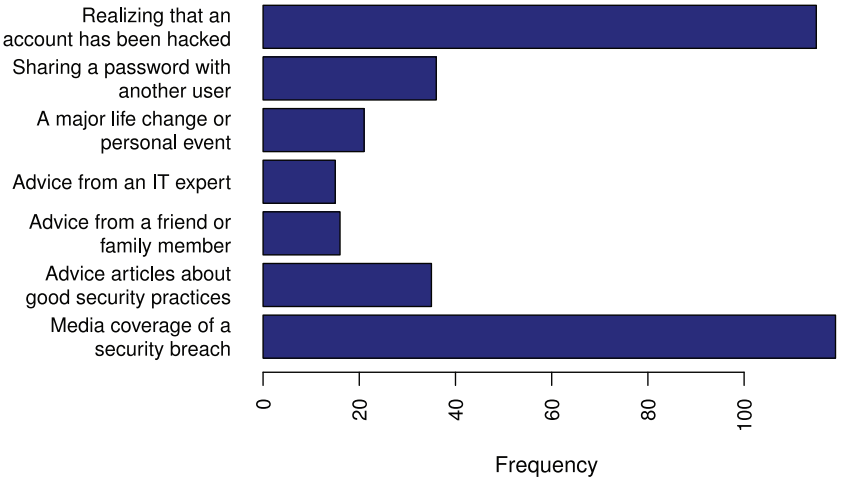

Fig. 7. Types of events that motivate users to change their passwords. Note that respondents were allowed to choose more than one option, so the bars do not sum to the number of respondents.

5.2.5 Changing Passwords. Only about one-third of respondents reported changing their passwords on a regular basis, but approximately two-thirds of respondents reported having changed their passwords in response to a specific event. In this case, the most common events were the compromise of an account and media coverage of a security breach (Figure 7).

The majority of respondents said that they forgot passwords at most once per month, and respondents were most likely to rely on the "forgot password" button (67%), followed by using the verification questions (44%) and guessing at the password (41%) in that situation. When respondents had to reset a forgotten password, respondents were most likely to say that they would change the password to what they thought it should have been (42% agreement), but in the case of forced password changes, they were most likely to say that their strategy was to choose an entirely new password (48% agreement).

5.2.6 Perceived Security Management. The final question group asked respondents to rate their agreement with a number of statements about how they ration their security efforts and perceive the task. The purpose of these questions was to investigate how respondents perceive the amount of effort devoted to password management and the success of these efforts. Because we did not think that users were conscious of their own rationing, we did not explicitly use the term *rationing* or *budgeting*, but the questions were aimed at understanding how users ration their own efforts.

Figure 8 shows responses to a series of Likert scale questions about respondents' perceptions of their security behaviour. Respondents were generally quite positive about password management: Of respondents, 55% agreed that picking new passwords was easy for them, and only 35% of respondents agreed that it is difficult to keep track of passwords. Most respondents indicated that they believed they were adequately protecting their accounts and felt that their accounts were unlikely to be attacked. However, the majority of respondents agreed that they could do more to protect their accounts. Surprisingly, 72% of respondents disagreed with the statement "I do not have time to pay attention to security."

Of respondents, 55% agreed that they had changed their password management strategies over time, showing evidence for the life cycle theory. Respondents were split on their perceptions of how they had reused passwords: Of respondents, 40% indicated that they had reused passwords

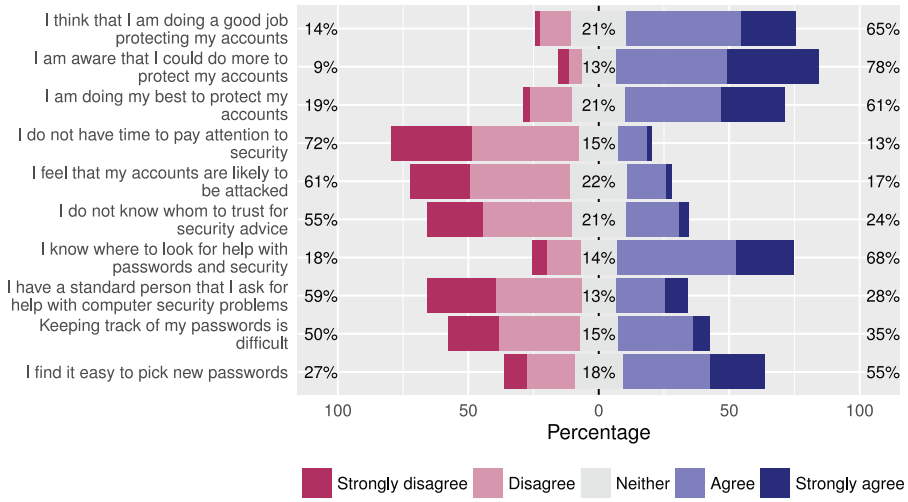

Fig. 8. Rating scales showing perceptions of difficulty of security tasks.

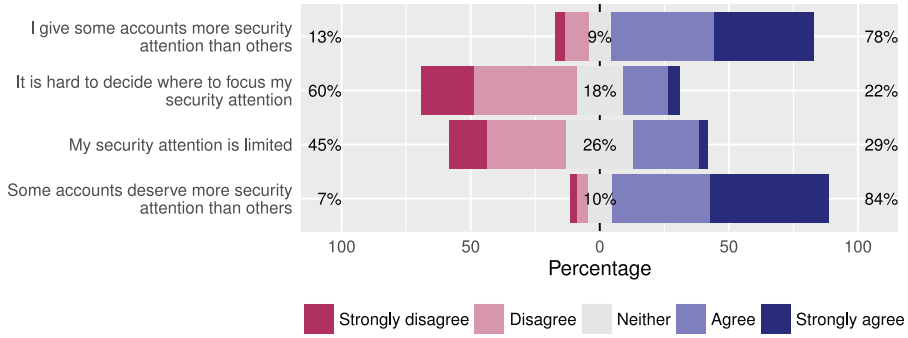

Fig. 9. Rating scales showing perceptions about attention paid to security.

from high-security accounts on low-security accounts, and 31% indicated that they had done the opposite. Both of these kinds of reuse can be a major threat to the security of high-importance accounts, because users may be less careful about the security of low-importance accounts. Forty-three percent said that they had shifted passwords from one account to another by choosing a new password for a high-security account and then reusing the old password on other accounts.

Figure 9 shows responses to Likert scale questions about "security attention." We chose not to define this term in the questions (although we did put it in quotes for special consideration) and left respondents to interpret it as their personal accumulation of time, attention, knowledge, education, and so on. Respondents indicated that they do ration security attention differently to different accounts: The majority of respondents agreed that they give more security attention to certain accounts and that some accounts deserve more security attention than others. Respondents did not seem to strongly agree that distributing security attention was a problem: Only 29% of respondents agreed that their security attention was limited, and only 22% agreed that they had trouble deciding where to focus their security attention.

5.3 Support for the Life Cycle

We analyzed our survey results to look for consistency with the life cycle model. In particular, we were looking for evidence that users reuse parts of passwords and systematic password management strategies, that they adapt their password coping strategies based on previous experiences from one account to another, and that they allocate resources differently to different accounts. We were also looking for similarity in reported numbers of passwords and rates of reuse as evidence that survey respondents were not (for example) creating unique passwords for every individual account. While not a strict validation, our goal was to confirm that the general patterns of use described in the interviews were present in the survey data.

Our survey results support the life cycle model. We found evidence of consistent strategies for password creation and reuse, as well as evidence that passwords are cycled through and modified for different accounts. Many respondents reported always or often including a specific type of personal information in passwords, and half of all participants reported using a consistent symbol, digit, or capitalized letter in their passwords. Participants also described consistent password reuse.

An important aspect of the life cycle is that even as time passes, parts of passwords and habits are maintained. We found strong support for this: The majority of survey respondents reported having a primary password and using it (or variations of it) on multiple accounts. Respondents said that they often included part of another password in new passwords, and when they change passwords, they often maintain part of the previous or another existing password. Respondents also reported "retiring" passwords by creating a new password on a high-security account and then reusing the old password on other accounts.

Our respondents did not seem discouraged by the tasks of password management. This was surprising to us, both because it differs from the impressions given in the interviews and because it differs from the popular culture surrounding passwords. It is difficult to know why these survey results are different. One possibility is sampling bias; perhaps our survey description attracted respondents who felt attentive to and confident about security, thus skewing the results. It is also possible that respondents tried to tell us what they thought we wanted to hear (a variation of the Hawthorne effect) or were embarrassed to admit that they had difficulty with these tasks. Gender differences in the three samples may also have affected the manner in which participants chose to disclose problems. We were not able to foster the same non-judgmental atmosphere in the survey as in the interviews, and this may have also affected participants' disclosure. Another possibility is that this is a more accurate representation of attitudes towards passwords and that the stories most often heard anecdotally are those of the proverbial "squeaky wheel," where the unhappiest users are heard the loudest.

We found evidence of rationing in the survey results but less strongly than we had expected. There was evidence that users supported the division of resources: Most respondents agreed that they gave some accounts more attention than others and that some accounts deserve this extra attention. However, participants did not agree that this attention was limited, and a large majority disagreed that they had problems deciding where to focus their security attention. This was somewhat counter to the impressions given of password management in the interviews. Apart from respondents' perception of their own practice, it was clear that they did have different strategies for different accounts. Among respondents who reused passwords, many participants said that they did not reuse passwords on banking websites and online stores that saved credit card information. People clearly had different strategies for accounts with different financial significance.

We asked respondents to self-rate their computer security expertise, and 30% of respondents reported themselves as either knowledgeable or expert in computer security. In an exploratory analysis, we found only small differences in reported behaviour between experts and non-experts. Experts were less likely to report reusing passwords (63% vs. 80% of non-experts) and reported

higher rates of dedicated password manager use (28% compared with 12%). This supports our finding in Study 2 that experts rely on many of the same coping strategies as non-experts.

These results show that users are thoughtfully distributing their own efforts but do not perceive it as such. It is positive that users do not seem to view this rationing as a hardship but also seems to show a lack of situation awareness that could possibly have a negative impact on password management behaviours.

6 DISCUSSION

Our studies showed that users cope with passwords by reusing passwords, writing them down, and creating new passwords by making slight variations of older passwords. However, users combine these possibly insecure strategies with more careful habits for accounts where they are strongly concerned about security and ration their effort into accounts with higher importance.

6.1 Education

The life cycle theory suggests several ways in which we can better educate people about coping with passwords. Users' coping strategies are effective but involve security risks. It would help users to better understand when these risks are heightened and better strategies for these situations.

One of the emergent themes during the non-expert interviews was confusion about threat models and the nature of the threat. Although worried about security, participants seemed unclear about the type of threats that concerned them. They did not differentiate among targeted personal attacks, anonymous large-scale password hacks, and the loss of private data, although they referenced all three during the discussions. Correspondingly, participants did not seem to appreciate that the defences for different attacks might vary based on the nature of the account in question. For instance, the password protecting an email account from an online attack addresses a different threat model than the PIN code stopping strangers from reading their email on a mobile device. This lack of understanding has an impact on how users ration their password efforts. If they are confused about the type of threat, then they may misdirect their efforts, leaving valued accounts unprotected and over-protecting less vulnerable accounts.

Our interview participants frequently expressed shame and embarrassment about their password habits. This seems to stem from the way that security advice is often presented without any contextual acknowledgement of the significance and quantity of accounts. Herley [24] points out that if users were to follow all given advice, then the security benefits would be swamped by the time spent following the advice. When providing security advice, the message needs to convey that coping strategies such as password reuse are appropriate to many accounts and that the important tactic is to carefully identify higher-importance accounts and direct extra effort toward them.

We suggest that end users should be able to develop consistent strategies to strongly protect the accounts they care about most, while not wasting effort on other accounts. The process of setting up a password manager can be daunting, but by selecting a small set of accounts for initial setup, the task is made significantly smaller. For example, users could select three important accounts, install a password manager, and add those accounts to the manager. Instead of attempting to solve their whole password problem, users could focus on the accounts that matter most to them. This incremental approach is scaleable, and it is possible that once a password manager is set up and in use, the user may want to use it for other accounts.

6.2 Design Recommendations

In addition to incorporating messages about sensible rationing into the advice delivered to users, the results of our studies and the life cycle theory suggest a number of ways in which the design of security products could better support users.

6.2.1 Writing Passwords Down. While writing passwords down is an intuitive and reasonable way of handling security, users need helpful guidance on the right way to store these passwords. Writing passwords down is conventionally understood to be insecure, but many security experts actually advocate writing passwords down [10, 35] if passwords can be kept in a physically secure location. Many users do write their passwords down, but the caveat about storage is poorly understood. In our studies, participants reported keeping their password lists in their email, in Dropbox, on their cell phones, or saved on their computer desktops. Recording passwords is a sensible way of conserving cognitive load, and users should be encouraged to make the small changes that could make this habit safer.

To address the storage problem and guide users to safer password storage, a plausible solution might be the development of a service specifically for secure password storage. Password storage notebooks do exist (e.g., The Personal Internet Address & Password Log Book [32]), but there is no equivalent online service. In the absence of a trustworthy electronic service, it seems possible to better emphasize the notion of physical security of stored passwords to users and suggest secure and sensible places to keep lists of passwords, such as in a locked desk drawer or a safety deposit box.

6.2.2 Password Managers. We were surprised to find that none of our non-expert participants used a dedicated password manager and that few were using browser-based password managers. As long as they are securely designed, password managers seem to offer one of the best solutions for password management: comprehensive, convenient, and safe. However, most of our non-expert participants appeared unaware of prominent password managers, and some expressed distrust in this software. We suggest that the better integration of password managers into operating systems and browsers would help with both visibility and trust. The advantage of password managers is that they are controlled by the user and can be used without changes to existing websites (unlike single sign-on). A well-integrated and usable password manager would let users ration effort into a mechanism that genuinely kept them safer.

Additionally, password managers create a central place through which passwords are created, saved, and monitored, and this could potentially help end users' situation awareness of their own passwords. Password managers provide users with a list of all their passwords, so users can see where they are reusing passwords, and in the case of a known vulnerability, make it easier for users to change affected passwords. Password managers could also help users by bringing vulnerabilities and compromises to users' attention. Some commercial password managers already do this: 1Password provides a service called Watchtower that allows users to identify services that are vulnerable to Heartbleed [3], and LastPass has a "Security Audit" feature that identifies passwords that occur in leaked datasets [18].

6.2.3 Extra Information. Throughout the interviews, participants referenced a lack of information about their passwords and accounts. When discussing suspected vulnerabilities, even experts expressed uncertainty about the status of accounts and the absence of information in situations such as Heartbleed. This lack of feedback is an inherent characteristic of security because helpful information cannot be made available to attackers but often-seen strategies such as obscuring the password policy do little to discourage attackers, while complicating the situation for end users. Additional information that could help users might include log information about sign-ins and actions, as well as information about security policies and password creation rules.

7 CONCLUSION

In this article, we presented three studies to investigate how users cope with the difficulties of living with passwords. We found that users have complex coping strategies that combine a

variety of tactics. They ration effort to devote resources to accounts they feel of greater importance and minimize their effort for accounts of lesser importance. Over time, this leads to a life cycle of password usage whereby passwords are developed, reused, adapted, discarded, or forgotten.

Password management can be a struggle for everyone, even experts in computer security. Our interviews with experts about their password management habits showed that they use a combination of password management strategies to carefully allot appropriate security to individual accounts. Several experts relied on password reuse and other less-secure coping strategies for lower-value accounts but used a password manager to generate and remember random passwords for high-security accounts. Experts' increased situation awareness allowed them to more easily make informed decisions about their password management tasks.

Finally, we conducted a quantitative survey about coping with passwords and found evidence that a broader population relies on the same kinds of coping strategies for password management as our interview participants. Respondents in our survey reported having systematic ways of creating passwords, reusing passwords for convenience and memorability, and creating variations on a "go-to" password to use on different accounts. Respondents divide their attention among multiple accounts and agree that some accounts deserve more attention than others. However, survey respondents did not report being as troubled by the demands of passwords and the difficulties of coping with them as the interview participants.

The results of the expert interviews and the survey support the life cycle theory that users are thoughtfully distributing their own efforts and that fragments of passwords and management strategies are cyclically reused from account to account, changing slightly in the process. However, the survey respondents described these resources as less stretched than the participants in Study 1 and were less negative about both the burden of the management task and the challenges of alloting resources. This may mean that our core code of rationing was mischaracterized. Although participants in all three studies described differently rationing password management resources to accounts with different needs, the survey participants appeared less frustrated by the decisions inherent in this rationing. If so, then this is a positive result, and we would like to think that users are not stressed by the work involved in this sensible password management task. Even if the management task is less difficult that suggested by the initial interview data, we still think there is room to improve the design of password systems and security technologies to incorporate the implications of the password life cycle to better support users.

Of course, we acknowledge that there can be dangerous security implications to password reuse and other coping strategies described here. Reusing whole passwords or pieces of passwords can make it easier for an attacker to gain access to multiple accounts once the password for one is guessed. Recorded passwords can be lost or stolen. However, these kinds of threats are personal, and many attacks are impersonal. Often, attackers want access to *an* email account, not *a particular* email account.

The contribution of this work is the identification of important patterns underlying user coping strategies. Users are not stubbornly refusing to follow password advice, they are instead carefully managing their resources to cope with impossible demands. Their solutions are often flawed, but they deserve consideration and may indicate better strategies for security. In choosing where to build roads, it may be best to pave the paths that users already walk.

REFERENCES

[1] Anne Adams and M. Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46.

[2] Anne Adams, M. Angela Sasse, and Peter Lunt. 1997. Making passwords secure and usable. In *Proceedings of HCI on People and Computers XII (HCI'97)*. Springer-Verlag.

[3] AgileBits. 2015. 1Password Watchtower. Retrieved from https://watchtower.agilebits.com.

[4] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security practices for households bank customers in the kingdom of saudi arabia. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*. USENIX, 297–308.
[5] Amazon.com, Inc. 2015. Amazon Mechanical Turk: Artificial Artificial Intelligence. Retrieved from https://www.mturk.com/mturk/welcome.
[6] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. 2007. Mental models of security risks. In *Financial Cryptography (FC)*. Springer, 367–377.
[7] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2009. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2009 Workshop on New Security Paradigms*. ACM, 47–58.
[8] Joseph Bonneau. 2012. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*. IEEE, 538–552.
[9] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qual. Res. Psychol.* 3, 2 (Jan. 2006), 77–101.
[10] William Cheswick. 2013. Rethinking passwords. *Commun. ACM* 56, 2 (Feb. 2013), 40–44.
[11] Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. 2006. A usability study and critique of two password managers. In *Proceedings of the 15th USENIX Security Symposium*. USENIX, 1–16.
[12] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse. In *Network and Distributed System Security Symposium*. The Internet Society, San Diego, CA.
[13] Paul Dourish, Rebecca E Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: User strategies for managing security as an everyday, practical problem. *Pers. Ubiq. Comput.* 8, 6 (Sept. 2004), 391–401.
[14] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my password go up to eleven?: The impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2379–2388.
[15] Mica R. Endsley. 1988. Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 97–101.
[16] Mica R. Endsley. 2006. Expertise and situational awareness. In *The Cambridge Handbook of Expertise and Expert Performance*, K. Anders Ericsson, Neil Charness, Paul J. Feltovich, and Robert R. Hoffman (Eds.). Cambridge University Press, Cambridge.
[17] K. Anders Ericsson. 2006. An introduction to the cambridge handbook of expertise and expert performance. In *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, Cambridge, 3–20.
[18] Jason Fitzpatrick. 2013. How to Run a Last Pass Security Audit (and Why It Can't Wait). Retrieved from http://www.howtogeek.com/176038/how-to-run-a-last-pass-security-audit-and-why-it-cant-wait/.
[19] Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proceedings of the International World Wide Web Conference (IW3C2'07)*. 657–666.
[20] Dinei Florencio, Cormac Herley, and Paul C. van Oorschot. 2014. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proceedings of the 23rd USENIX Security Symposium*. USENIX, 575–590.
[21] Shirley Gaw and Edward W. Felten. 2006. Password management strategies for online accounts. In *Proceedings of the 2nd Symposium on Usable Privacy and Security*. ACM, 44–55.
[22] Leo A. Goodman. 1961. Snowball sampling. *Ann. Math. Stat.* 32, 1 (Mar. 1961), 148–170.
[23] Eiji Hayashi and Jason Hong. 2011. A diary study of password usage in daily life. In *Proceedings of the International Conference on Human Factors in Computing Systems*. ACM, 2627–2630.
[24] Cormac Herley. 2009. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms*. ACM, 133–144.
[25] Iulia Ion, Robert W. Reeder, and Sunny Consolvo. 2015. "...No one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*. USENIX.
[26] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*. USENIX.
[27] Kenneth J. Knapp, Thomas E. Marshall, R. Kelly Rainer, and F. Nelson Ford. 2006. Information security: Management's effect on culture and policy. *Inf. Manage. Comput. Secur.* 14, 1 (Jan. 2006), 24–36.
[28] LastPass. 2016. LastPass: Simplify Your Life. Retrieved from http://lastpass.com.
[29] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie Calvin Xu. 2009. Studying users' computer security behavior—A health belief perspective. *Decis. Supp. Syst.* 46 (2009), 815–825.
[30] Donald A. Norman. 2009. When security gets in the way. *ACM SIGCSE Bull.* 16, 6 (Nov. 2009), 60–63.
[31] Gilbert Notoatmodjo. 2007. *Exploring the 'Weakest Link': A Study of Personal Password Security*. Master's thesis. The University of Auckland, New Zealand.

[32] Peter Pauper Press. *The Personal Internet Address & Password Log Book (Organizer)*. Peter Pauper Press.
[33] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS'12)*. ACM.
[34] Carsten Schmitz. Accessed 2015. Limesurvey—The Free and Open Source Survey Software Tool! Retrieved from https://www.limesurvey.org/.
[35] Bruce Schneier. 2005. Write Down Your Password. Retrieved from http://www.schneier.com/blog/archives/2005/06/write_down_your.html.
[36] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle M. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the 6th Symposium on Usable Privacy and Security*. ACM.
[37] Herbert A. Simon. 1977. The structure of Ill-structured problems. In *Models of Discovery*. D. Reidel Publishing, Dordrecht, 304–325.
[38] Michelle Steves, Dana Chisnell, M. Angela Sasse, Kat Krol, Mary Theofanos, and Hannah Wald. 2014. *Report: Authentication Diary Study*. Technical Report. National Institute of Standards and Technology, Information Technology Laboratory, Gaithersburg, MD.
[39] Elizabeth Stobert and Robert Biddle. 2014. The password life cycle: User behaviour in managing passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS'14)*. USENIX.
[40] Elizabeth Stobert and Robert Biddle. 2016. Expert password management. In *Proceedings of the International Conference on Technology and Practice of Passwords (PASSWORDS'15)*. Springer, 3–20.
[41] Anselm Strauss and Juliet Corbin. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2nd ed.). SAGE Publications, Thousand Oaks, CA.
[42] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2011. What makes users refuse web single sign-on?: An empirical investigation of OpenID. In *Proceedings of the 7th Symposium on Usable Privacy and Security*. ACM.
[43] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I added '!' at the end to make it secure": Observing password creation in the lab. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*. USENIX, 123–136.
[44] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2013. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Proceedings of the 14th International Conference on Human-Computer Interaction*. Springer, 460–467.
[45] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS'10)*. ACM.
[46] Rick Wash, Emilee J. Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding password choices - how frequently entered passwords are re-used across websites. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'16)*. USENIX.
[47] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*. ACM, 162–175.
[48] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and Nasir Memon. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.* 63, 1–2 (July 2005), 102–127.
[49] Moshe Zviran and William J. Haga. 1999. Password security: An empirical study. *J. Manage. Inf. Syst.* 15, 4 (1999), 161–185.

Received October 2016; revised October 2017; accepted January 2018