Fagan *et al. Hum. Cent. Comput. Inf. Sci.* (2017) 7:12
DOI 10.1186/s13673-017-0093-6

Human-centric Computing and Information Sciences

RESEARCH Open Access

An investigation into users' considerations towards using password managers

Michael Fagan[1*†], Yusuf Albayram[1†], Mohammad Maifi Hasan Khan[1] and Ross Buck[2]

*Correspondence: michael.fagan@uconn.edu
†Michael Fagan and Yusuf Albayram contributed equally to this work
[1] Department of Computer Science and Engineering, University of Connecticut, Storrs, CT, USA
Full list of author information is available at the end of the article

Abstract

Password managers, though commonly recommended by security experts, are still not used by many users. Understanding why some choose to use password managers while others do not is important towards generally understanding why some users do what they do and, by extension, designing motivational tools such as video tutorials to help motivate more to use password managers. To investigate differences between those who do and do not use a password manager, for this paper, we distributed an online survey to a total of 137 users and 111 non-users of the tool that asked about their opinions/experiences with password managers. Furthermore, since emotion has been identified by work in psychology and communications as influential in other risk-laden decision-making (e.g., safe-sex behavior such as condom use), we asked participants who use a password manager to rate how they feel for 45 different emotions, or, as the case for those who do not use a password manager, to rate how they imagine they would feel the 45 emotions if they did use the tool. Our results show that "users" of password managers noted convenience and usefulness as the main reasons behind using the tool, rather than security gains, underscoring the fact that even a large portion of users of the tool are not considering security as the primary benefit while making the decision. On the other hand, "non-users" noted security concerns as the main reason for not using a password manager, highlighting the prevalence of suspicion arising from lack of understanding of the technology itself. Finally, analysis of the differences in emotions between "users" and "non-users" reveals that participants who never use a password manager are more likely to feel suspicious compared to "users," which could be due to misunderstandings about the tool.

Keywords: Password manager, Adoption, Security, Usability, Emotion

Background

The proliferation of online services has drastically increased the number of passwords an individual user is required to remember to access different online accounts. For example, an average user is estimated to have 25 distinct online accounts [1], each with a password to manage and remember. While creating unique and strong passwords for each online account and never recycling from service to service is essential for security, the cognitive burden of remembering so many unique and complex passwords is becoming

increasingly challenging for users. To address this, password managers are often recommended by security experts as a convenient solution [2] that can help users pick passwords (i.e., with unique, random generation features) and store them securely in an encrypted form without requiring users to remember all of their passwords.

Interestingly, despite being frequently advised by security experts [3–8], many users choose not to use password managers. Designing persuasive campaigns (e.g., video tutorials) that can motivate users to adopt such tools can be an effective way to address this challenge, but before such persuasive campaigns can be designed, we argue that it is important to investigate and understand several aspects of the decision-making process behind using or not using password managers. To address this void and gain insight into users' considerations regarding the use of password managers, in this study, we investigate answers to the following research questions:

1. Is there any difference between users and non-users in terms of demographics and the level of self-reported computer proficiency?
2. What are the main reasons behind using password managers?
3. What are the main reasons behind not using password managers?
4. Is there any difference between users and non-users in terms of concerns about computer security?
5. Does the number of online accounts change the perception of password managers' utility?
6. Is there any difference in the emotions they feel/experience when users' use and non-users anticipate using password managers?

Our first four research questions address differences between users and non-users of password managers, specifically in their composition, experience, and attitude. The findings here will be helpful towards identifying strategies for reducing non-users' concerns with password managers. For example, if many non-users do not see the benefit of using the tool, then this concern can be addressed in future interventions. Additionally, by understanding who uses a password manager and why they choose to use the tool, we can possibly understand how some individuals become password manager users. Prior work has drawn attention to the issue of cognitive burden felt by users around account security and how this can lead to non-compliance [1]. Thus, the fifth research question tests if those who are expected to experience more cognitive burden (due to more accounts) are more likely to adopt a password manager. By exploring this area, we can further identify motivations of users of the tool with the hopes of leveraging those findings towards encouraging adoptions among non-users. Finally, our sixth research question incorporates the growing track of psychology and communications literature that calls for attention to the emotional context of risk associated decisions [9]. By identifying differences in emotions between groups, strategies for dealing with the emotions felt by non-users that can inhibit adoption can be devised.

To answer the above questions, we designed and conducted an online survey distributed to a total of 248 Mechanical Turk (MTurk) users and collected users' opinions/experiences with password managers. In addition to asking participants about the reasons behind their decisions, to better understand the differences in emotions between

users and non-users, which can also influence their behavior outcome and explain the differences in adoption rate, we collected ratings for and analyze the strength of emotions (e.g., happy, sad, confident, nervous) participants report they might feel when using their password manager or, in the case the participant does not use the tool, the strength of emotions participants report they think they would feel if they were to use the tool.

Our study considers several variables: concern regarding computer security, user's online behavior and attitudes, attitude towards password managers, reasons for using or not using a password manager, emotions elicited by the usage of password managers for users, and emotions elicited by anticipated usage of password managers for non-users. All of these variables are defined in our study using survey instruments and self-reported ratings that reflect each. Details of variable definitions can be found in Methods.

To perform comparative analysis, in our study, we categorized the participants as "users" (i.e., those who have used a password manager) and "non-users" (i.e., those who have not used a password manager), and investigated differences between the two groups. This study makes the following key contributions. *First*, we find "users" rate their computer proficiency and computer security ability higher than "non-users", but overall both groups were similar in their responses to instruments not directly related to password managers. *Second*, based on quantitative ratings, "users" generally find password managers more useful, convenient, and secure. On the other hand, "non-users" do not generally see password managers as an effective way to manage their passwords. *Third*, in qualitative comments, "users" mention convenience and usefulness as the main reasons for using a password manager and find that the more accounts they have, the more useful they think password managers are, while "non-users" note security and usability issues as the chief reasons for not using a password manager and mention being worried about putting all of their passwords in a single place. *Finally*, analysis of differences in emotions between "users" and "non-users" reveals that participants who use a password manager are more likely to feel secure, admiring and energetic, and less likely to feel suspicious when using their password manager to log into a website.

These findings suggest that there could be a lack of understanding about how password managers work and that even users of the tool may not understand the security benefits of their decision. Any effort which attempts to persuade users to adopt password managers needs to clearly explain the purpose of the tool and the technology behind it, which can reduce users' misunderstandings, thereby hopefully reducing feelings of suspicion. It is possible that better education about the security benefits of password managers and similar tools, even directed towards current users could help increase adoption. The importance of convenience to users of password managers and the relatively high adoption rate of password managers show the power that usable tools have towards motivating secure behavior, even if the users do not necessarily know they are being secure. Our emotion findings highlight how complex feelings of trust and motivation to be secure are intertwined and suggest that cultivating the positives (e.g., energetic, secure) and reducing the negatives (e.g., suspicion) around password managers can further help increase adoption.

The rest of the paper is organized as follows. The background work related to our study is presented and explained in the context of the research questions in "Related work" section. The study's design and procedures are detailed in "Methods" section. We

present the findings of our study in "Results" section. Finally, the results are discussed with connections to prior work in "Discussion" section, and the paper is concluded.

Related work

Password reuse has been identified as a common [1], but troubling user behavior that leaves many vulnerable to a broad range of attacks [10, 11]. To address this problem, password managers are designed to reduce or eliminate password reuse across multiple accounts and devices through lightweight password generation and management features that allow users to create random, unique passwords across their accounts while only needing to remember the password to their password manager to access those accounts. If properly utilized, a password manager can help users stay secure without increasing their cognitive burden through arduous memorization, and so many experts recommend users take up the tool [2, 8]. Thus, this study investigates what users think of these tools towards understanding why some choose to use them while others do not.

In analyzing password managers, our work follows from several prominent prior studies. Chiasson et al. is one of the closest in spirit to our's, where the authors conducted a usability study of two password managers (PwdHash and Password Multiplier) [12]. In both cases, they identified several usability issues caused by: (1) users' mental models (i.e., incomplete understanding of the tool) and (2) users' view on the necessity of the tool (e.g., users do not feel that they need a password manager). In another effort, Karole et al. presented a comparative usability study of three password managers (LastPass, KeePassMobile and Roboform2Go) in terms of security, ease of use, necessity and level of acceptance. They found that users were not comfortable giving control of their passwords to an online manager (e.g., LastPass) and preferred to manage their passwords on their mobile devices (e.g., Roboform2Go), despite the better usability of the online manager [13].

The studies described above focused on the usability of password managers, but the study presented here focuses more on user perceptions and opinions about the tool, rather than directly assessing usability. This divergence is inspired by the growing literature in the cybersecurity field relating to user's psychology and perceptions [14–16]. Herely has published multiple papers regarding the possible misalignment of security tools' benefits with what users need, drawing attention to the importance of users' perceptions in their decision-making [15, 16]. User-centeredness has grown as a goal in many circles within the usable security field [17, 18]. This has drawn others in more recent studies to focus on user-centered approaches meant to alter perceptions of a decision. Harbach et al. in 2014 showed that adding explicit personal examples of how Android permissions can impact a user (i.e., if an app is allowed access to the camera, it can take photos) made participants pay more attention to these permission requests [19]. Das et al. showed that social influences were key in users' consideration of security decisions and impactful towards security outcomes [20]. Several studies have identified the importance of individual considerations in the decision of users to apply a software update [21–24]. In particular, past experiences were identified to be an important factor in users' decisions, particularly if past experiences were negative [22, 23]. In addition to user perceptions, more work in cybersecurity is also taking a more

explicitly psychological approach towards understanding users' computer security behaviors, as shown in Howe et al.'s 2012 survey of literature related to the psychology of end-users [25].

Other than the general user-centric approach to the design presented in this paper that focuses on users' perceptions and psychology, our work is also heavily motivated by prior work which has argued that emotions are an important aspect of decision-making and can influence it in multiple ways [9, 26]. Other than investigating the underlying rationale behind users' decisions, we look into emotional differences between "users" and "non-users." For example, in the context of password managers, we argue that if a user believes that password managers are not reliable/secure, this can evoke emotions of suspicion, and can indeed lead to non-adoption. Also, if someone is not proficient in using computers, they may be more reluctant to adopt new tools as doing so requires learning something new, which can evoke anticipatory emotions of frustration and anxiety [27]. Such emotions can also lead users to rationalize their actions (e.g., non-adoption) in a more logical light. For instance, someone may justify not using a password manager by simply thinking "I do not need one," which could hide irrational reasons for avoiding the tool (i.e., frustration, anxiety) with rational alternatives, in this case the lack of need for using the tool. On the other hand, the possibility of losing access to one's online accounts can evoke fear, which can motivate one to take actions if the level of fear is strong enough. Other work has looked at emotions of users when using computers, notably Kay and Loverock's study to develop a scale for the emotions when using new software, which found that, among other findings, ratings of anxiety and happiness as a result of using new software were significantly correlated with increasing computer knowledge among students taking an 8-month computer laptop and software class [28].

Motivated by the work described above, our study was designed to investigate users' perceptions of password managers, as well as their emotional response to using the tool. Specific survey instruments were adapted from prior work, including Ion et al.'s study comparing behaviors of expert and non-expert users, Stobert and Biddle's investigation of how users manage passwords, as well as Stobert's work on graphical passwords and password management [8, 29, 30].

Methods

Survey design

To understand the reasons for using or not using password managers and investigate users' security behavior and opinions related to password managers, we conducted an online survey using Amazon's MTurk. In the survey, participants first answered demographic questions and then questions about computer and online security behavior. Participants were asked if they know what a password manager is and if they have ever used it. These questions served as branching questions and based on the answer, participants were categorized into two groups: (1) those who have used a password manager (i.e., "users") and (2) those who know what a password manager is, but have never used it (i.e., "non-users"). Groups were directed to branches as follows.

All participants were shown a grid of statements about their general computer security experience and attitudes, followed by another grid about password managers. They were asked to indicate their level of agreement with each statement on a scale of 1 =

"Strongly disagree" to 5 = "Strongly agree." The survey instruments were designed based on prior research and modified accordingly. All survey instruments can be found in the "Appendix".

In addition to asking their reasons behind their decisions regarding the use of the tool, to better understand how "users" and "non-users" differ in terms of emotional response to the possibility of using password managers, participants were asked to rate how they might feel 45 different emotions (on a scale of 1 = "Never" to 5 = "All the time") while using the tool. These emotions were chosen to cover the broad range of responses one could have while using a tool/software on a computer. The question about each emotion was shown to participants *in random order*, one question at a time to avoid biasing them. Questions were presented in the format "One might feel [*Emotion*]." The list of emotions can be seen in Table 9 in the "Appendix". Please note that "users" were asked to report their emotions when using a password manager, while "non-users" were asked to imagine they used a password manager and to report the emotions they *would* feel in doing so. Prior work, including our own, has found that past experiences, along with other user-centric clues are very important to individuals' considerations and their decisions' expected outcomes. Thus, we compare "non-users" expected experience while using a password manager with "users" self-reported history with the tool to help explain the groups' divergent outcomes.

Finally, we asked open-answer questions about the reasons participants may have for using or not using a password manager. Specifically, "users" were asked *"Why do you choose to use a password manager?"*, while "non-users" were asked *"Why do you choose not to use a password manager?"*

Definition of variables

Our study considers several variables that cover participants' overall computer security experience as well as their password manager specific attitudes and experiences. Specifically, we incorporate the following variables: concern regarding computer security, user's online behavior and attitudes, attitude towards password managers, reasons for using or not using a password manager, emotions elicited by usage of password managers for users, and emotions elicited by anticipated usage of password managers for non-users. Concern regarding computer security is measured using self-reported ratings of agreement with the statements presented in Table 7 (adopted from [30]). Attitudes towards password managers in general are measured using self-reported agreement ratings for statements presented in Table 8 (adopted from [30]). Participants' reasons are ascertained through qualitative coding of each participant's open-answer comment about their decision. Emotions are measured for 45 different emotions as listed in Table 9. For sake of space, these tables are all located in the "Appendix", which contains the rest of the survey language used.

Procedure

The survey was restricted to MTurk participants who are 18 years of age or older, currently living in the United States, have a HIT (Human Intelligence Task) approval rate of 85% or higher, and have completed at least 1000 HITS/tasks. Each participant was paid

$1 for participation and was only allowed to participate once by an individual. The study was approved by the University's Institutional Review Board (IRB).

Results

We recruited a total of 248 paid participants to answer the survey used in our study. We removed 2 responses from users who answered branching questions inconsistently (i.e., said they used a password manager, but also did not know what a password manager is). Table 1 shows the percentage of participants who are either "users" or "non-users." As can be seen in the table, we have an almost equally balanced number of "users" and "non-users" where 55% of participants were "users" and 45% of participants were "non-users." Using our variables as a guide, we explored differences between these groups.

Differences in computer proficiency between "users" and "non-users"

Based on our data, we found that male participants adopt password managers more than female participants ($\chi^2 = 6.25$, $df = 1$, $p = 0.012$). Specifically, 65.7% of the users were male and 33.6% were female. By contrast, 50.5% of "non-users" were male and 49.5% were female. Also, participants who say they use password managers are more likely to rate their computer proficiency higher. A Mann–Whitney U test shows that there is a significant difference in the level of computer proficiency between "users" and "non-users" ($U = 6175$, $p = 0.008$). Responses for gender and self-reported computer proficiency are also found to be significantly correlated with each other using Spearman's coefficient [31] ($\rho = -0.307$, $p < 0.001$), with males rating their proficiency significantly higher in general than females ($U = 4823$, $p < 0.001$). Since our groups (i.e., "users" and "non-users") are independent and the response data is ordinal, but we do not have confidence in the normality of our underlying distributions, we use non-parametric tests like Mann–Whitney U tests for our analysis [32].

In addition to asking participants about their computer proficiency, we presented another set of statements asking about their computer security knowledge. Table 2 shows these statements along with average response for each group and the significance test between these distributions. The biggest takeaway from this table is that participants

Table 1 Demographics across the two groups (i.e., "users" and "non-users")

	Participants ($n = 248$)	
	Users ($n = 137$)	**Non-users ($n = 111$)**
Gender		
Male	90 (65.7%)	56 (50.5%)
Female	46 (33.6%)	55 (49.5%)
Rather not say	1 (0.7%)	0 (0%)
Age		
18–25	31 (22.6%)	31 (27.9%)
26–34	59 (43.1%)	41 (36.9%)
35–54	41 (29.9 %)	30 (27.0%)
55–64	6 (4.4%)	9 (8.8%)
Overall	55%	45%

Percentage of participants in each group is also shown

Table 2 Respondents to the password manager survey were asked to agree with each statement on a scale of 1 = "Strongly disagree" to 5 = "Strongly agree"

Statement	Users	Non-users	U test	
	Mean (med.)	Mean (med.)	*U*	Sig.
I am doing a good job of protecting my computer security	4.05 (4)	3.77 (4)	6241	0.005
I could do more to protect my accounts	3.56 (4)	3.68 (4)	7352.5	0.628
I do not have time to pay attention to security	1.96 (2)	2.09 (2)	7030.5	0.266
I do not feel my accounts are likely to be hacked	3.23 (3)	3.15 (3)	7100	0.472
I do not know where to get computer security advice	1.83 (2)	2.08 (2)	6603	0.084
I am knowledgeable about computer security	3.91 (4)	3.64 (4)	6469	0.031
I care about computer security	4.16 (4)	4.19 (4)	7297	0.625
I trust my computer	3.66 (4)	3.72 (4)	7315.5	0.58

Average and median response rating for each group is shown along with the resulting *U* statistic and significance value of a Mann–Whitney U test comparing responses for each statement between the groups

who have used password managers indicate that they agree with the statement "I am doing a good job of protecting my computer security" significantly more ($U = 6241$, $p < 0.006$) than "non-users." There is also a significant difference in agreement with the statement "I am knowledgeable about computer security" between the groups, with "users" rating their agreement with that statement as higher than "non-users." Interestingly, there are no significant differences between the groups for statements like "I could do more to protect my accounts," indicating that while "non-users" feel they are not doing as good a job at protecting their computer security as "users," they do not feel they *could* be doing more, which is interesting as it points to one possible reason why they choose not to use password managers. Specifically, even though some want to improve their security, they do not see password managers as an effective way to do this, indicating their lack of understanding regarding the security benefit of the tool.

Though we did find some differences between self-report computer proficiency and agreement with a few statements, overall, the samples were fairly similar as demonstrated by the similar age range and similar agreements with most statements. Differences in proficiency and computer security knowledge could be due to "users" actually have more proficiency and knowledge than "non-users," but the higher ratings for "users" could also be due to an inflation in their ratings due to them currently using a password manager. "Users" may *think* they are better at security due to their use of a password manager, but they are in fact no more proficient or knowledgeable than "non-users."

Differences in opinions about the tool between "users" and "non-users"

To determine possible differences in opinion about password managers between "users" and "non-users," participants were shown a set of statements (Table 3) and were asked to rate on a scale of 1 = "Strongly disagree" to 5 = "Strongly agree" how much they agree with each statement.

As can be seen in Table 3, there are significant differences in the ratings for multiple statements regarding security and usability aspects of password managers between "users" and "non-users." For example, while both groups report similar agreement with the statement "I understand the theory behind password managers," "users" agree significantly more with the statement about understanding why password managers are

Table 3 Participants were asked to agree with each statement regarding password managers on a scale of 1 = "Strongly disagree" to 5 = "Strongly agree"

Statement	Users	Non-users	U test	
	Mean (med.)	Mean (med.)	*U*	Sig.
I trust password managers	3.77 (4)	3.05 (3)	4422.5	<0.001
Password managers are more secure	3.58 (4)	2.98 (3)	5125	<0.000
Password managers help people	4.28 (4)	3.85 (4)	5231.5	<0.001
Password managers are easy to use	4.19 (4)	3.87 (4)	5742	<0.001
Password managers are more convenient	4.16 (4)	3.84 (4)	5966	0.002
I understand the theory behind password managers	4.14 (4)	3.89 (4)	6606.5	0.053
I understand why password managers are secure	3.78 (4)	3.05 (3)	4580	<0.001
I worry that accessing my accounts may be more difficult with a password manager	2.31 (2)	2.69 (2)	6063.5	0.004

Average and median response rating for each group is shown along with the resulting *U* statistic and significance value of a Mann–Whitney U test comparing responses for each statement between the groups

secure. Also, "users" agree significantly more with the statements about password managers being more secure, easy to use, convenient and helpful. Moreover, "users" agree significantly more with trusting password managers compared to "non-users" and they are significantly less worried about having difficulty accessing their accounts while using a password manager compared to "non-users." Together, these results could suggest that those who use a password manager are more knowledgeable about password managers and its security, usability, and convenience benefits, possibly due to higher technical expertise, but their experience with the tool could also have led to their ratings. For example, when deciding to use a password manager, "users" may have done research, or in using the tool for some time, these participants may have learned about aspects of the tool that "non-users" may not be aware of.

Number of accounts matter only if the tool is tried

Next, we looked at the correlation between the number of accounts an individual has and their perceptions of password manager usefulness. Intuitively, if a person has more accounts, it is more likely that he/she may feel password managers to be more useful. To this end, we tested whether the usefulness of password managers are tied to the number of accounts/passwords owned or used by the participants.

We found that password manager "users" report having significantly more accounts ($U = 4887.5$, $p < 0.001$), using them more frequently ($U = 6096$, $p = 0.007$), and having more unique passwords ($U = 6247$, $p = 0.016$) than "non-users." Additionally, for "users," there are significant correlations between the number of accounts the participants report having and their rating of both how much they think password managers help people in general ($\rho = 0.223$, $p < 0.01$) and how much they think *their password manager* helps them personally ($\rho = 0.194$, $p < 0.05$). These correlations did not hold in significance for the "non-users" group of participants. This suggests that there is a relationship between the number of accounts an individual has and their perception of how useful a password manager is if they use it, but that relationship does not seem to exist in the minds of "non-users." Considering the function of a password manager, it makes sense that someone with many accounts will find that it helps them more than

someone with fewer accounts, but it seems to take experience with password managers to help "users" realize this connection. It is also possible that this relationship works in the other direction: those who realize that more accounts means more utility from a password manager and therefore begin to use one. The significant difference in the number of accounts between "users" and "non-users" further supports this relationship (by indicating that "users" do, in fact, have more accounts than "non-users").

Differences in underlying reasons for using or not using

In order to better understand the reasons for using or not using password managers, participants were asked, *"Why do you choose [not] to use a password manager?"* More specifically, participants who reported having used password managers were asked why they chose to do so. Conversely, those who have never used password managers, but have heard of them, were asked why they chose not to use the tool.

To analyze the open-ended responses, we used an inductive coding approach [33]. One author developed the initial codebook and performed the initial pass of coding. Another author further developed the codebook and reviewed coding. Finally, a third author reviewed the final codebook and agreed with the codes applied by the prior two authors. Table 4 shows the results of the coding of reasons for using or not using a password manager. Please note that the numbers do not add up to 100% since a participant's response can be related to multiple reasons.

Coding revealed that the chief reasons for using password managers as reported by participants who use a password manager are usability and convenience. Usability and convenience benefits of password manager are mentioned in 80% of the comments from "users." Example benefits include the functionalities password managers provide such as helping them securely store passwords without having to remember them and ease of access to websites (e.g., auto filling passwords). Security benefits are mentioned in 24.6% of comments as being an important factor for using a password manager, but 6 of those 15 also mentioned convenience in their response, showing that even many who acknowledge the security benefits note the convenience as well.

When it comes to "non-user" participants' reasons for not using a password manager, 45.9% of the comments note security concerns. Examples include fear of the password manager being compromised and finding it risky to put all of their passwords in one place which can fail (i.e., single point of failure). Interestingly, 42.3% of the comments indicate "lack of need" as one of the reasons for not adopting password managers, possibly suggesting a lack of understanding regarding the security risks and/or the benefits of the tool. Finally, 10.8% of the comments indicate lack of time/motivation as one of the reasons for not adopting the tool. Interestingly, none of those who said they had a lack of time/motivation also mentioned a lack of need in their comment, suggesting these reasons could be seen as mostly mutually exclusive in our case. Also, while only 1% of comments mention both security concerns with password managers and a lack of time/motivation, 8% of the comments that mention security also indicate a lack of need for a password manager. This could mean most that say they do not have the time or motivation to use a password manager, unlike others, do not necessarily see them as insecure. Unfortunately, at best this group is likely to be a minority of non-users since only 12 comments out of 111 total mention the lack of time/motivation as a reason at all. These

Table 4 Frequencies of codes in each category being applied to participants' reasons for using or not using password manager along with sample responses

	Reason	Count	Sample response
Users	Convenience	49 (80.0%)	*"Because I just have so many accounts that writing them down like I had been doing was just getting to be too much"*
			"To help me remember passwords"
			"It's convenient and easy to use"
			"Because it is hard to remember so many different passwords"
			"To remember complex passwords"
	Security	15 (24.59%)	*"It makes my password use more secure"*
			"More secure than trying to write passwords down and more accurate than having to remember passwords"
			"It's easier to manage all accounts. Complex passwords can also be generated and remembered in the service/program itself"
	Other	1 (1.6%)	*"Work related purposes"*
	Security concerns	51 (45.94%)	*"Single point of failure"*
			"I think that it is risky to have all of my passwords in one place, and I do not want to do it. I'd rather memorize them"
			"I feel they aren't secure"
			"I don't use it for sites I need the most security on, like my bank"
Non-users	Lack of need	47 (42.34%)	*"I can remember my passwords without the use of one"*
			"I start on PC in the mid 70s and from the start I use a book for login and passwords'"
			"I'm not sure. I just prefer to keep a variety of passwords and keep track of them on my own"
	Lack of time/motivation	12 (10.81%)	*"Haven't bothered to learn enough about it yet, too lazy I suppose"*
			"It's sometimes a hassle and I'm in a hurry"
	Inconvenience and usability concern	10 (9.0%)	*"It seems inconvenient"*

Please note that the numbers do not add up to 100% since a participant's response can contain multiple reasons

findings highlight that, while password managers are advertised and recommended as a secure way to manage passwords, users often do not adopt password managers due to security concerns and/or fail to see the benefit of the tool, highlighting the misunderstanding regarding the technology on users' part, possibly a consequence of low computer proficiency and/or poor communication on the part of software manufacturers and promoters.

Emotion

Motivated by prior work that has argued that emotions are an important aspect of decision-making [9], we analyze emotion ratings from "users" and "non-users." As a reminder, for emotion ratings, participants who say they use a password manager were asked to rate how they feel while using their password managers. Participants who say they do not use a password manager were asked to rate how they think they would feel

if they used a password manager. All participants (i.e., "users" and "non-users") were asked to rate how they might feel 45 different emotions (on a scale of 1 = "Never" to 5 = "All the time") while using a password manager. To better understand the differences in emotions (if any), first, we looked at correlations between emotion ratings and self-reported computer proficiency for "users" and "non-users." We used Spearman's correlation analysis and found strong correlations between level of computer proficiency and four emotions for "users." Similarly, we also performed the same correlation analysis for "non-users" to see if there is a correlation between emotions and self-reported computer proficiency for "non-users" when they imagine using a password manager to log into a web site. The results of the correlation analysis can be seen in Table 5.

As shown in Table 5, for "users," the higher the level of computer proficiency, the more likely they are to feel confident, secure, respectful, and friendly. Thinking to our other results, specifically the prevalence of convenience as a reason for those who use password managers to do so, this indicates that more proficient participants may have better understanding of the security benefits from password managers. We dug deeper into the "user" group data to better understand some of these emotions findings. Using Spearman's correlation analysis on the "user" data to determine relationships between emotion ratings and whether the comment form the participant mentioned a security benefit to using a password manager, we find significant correlations for two emotions: confident (ρ =0.282, $p = 0.028$) and respectful ($\rho = 0.360$, $p = 0.004$). For confident, this suggests that those who give more thought to the security benefits of the password manager they use (as suggested by them leaving comments that mention security) rate their confidence when using a password manager as higher, possibly because they feel more secure [though ratings of the emotion "secure" are not correlated with security reasons in comments ($\rho = 0.106$, $p = 0.417$)]. The stronger and more interesting relationship is with the emotion respectful. The survey instrument for respectful is "One might feel RESPECTFUL (e.g. because the system has given one tools to respond)," which may give insight into this correlation. It could be that those who are more mindful of the security benefits of password managers are more likely to *respect* the tool for helping them. Other emotions that used the same example phrasing (i.e., "because the system has given one tools to respond"), such as grateful, admiring, and trusting, do not show correlations with mentions of security benefits, showing that it was not just this prompt that was correlated, but the prompt combined with respectful specifically. Confidence and respect are positive emotions for participants to be feeling in this circumstance and so

Table 5 Spearman's ρ and significance values for correlation analysis between select emotion ratings and self-reported computer proficiency for for "users" and "non-users"

Emotion	Users		Emotion	Non-users	
	ρ	Sig.		ρ	Sig.
Confident	0.168	0.049	Powerful	0.196	0.039
Secure	0.168	0.049	Grateful	0.206	0.030
Friendly	0.174	0.043	Welcomed	0.224	0.018
Restpectful	0.178	0.039	Contemptuous	0.266	0.005

We highlight the most significantly correlated emotions to show the differences in this result between groups

encouraging these feelings, possibly through increasing awareness of password managers' security benefits is recommended.

When it comes to "non-users," the higher their level of computer proficiency, the more likely the participant is to highly rate feeling powerful, grateful, welcomed, and contemptuous. Like before, we dug into the "non-user" using correlation analysis combined with the qualitative codings to discover trends. Two emotions had significant correlations. Those who rate that they would feel grateful while using a password manager lower are more likely to say in their comments that they lack time or motivation to use a password manager ($\rho = -0.212, p = 0.025$). Considering that our study prompted "non-users" to imagine they used a password manager, this finding is fairly logical since those who do not feel they have time to use a tool would be *ungrateful* for having to use one. It could also be that the participants are not grateful for the tool because they do not think it is useful or important, which could also be why they said they had a lack of time or need for it. Ratings for feeling powerful are also correlated with two sets of codes on comments: lacking time/motivation ($\rho = 0.205, p = 0.031$) and not having a need for a password manager ($\rho = -0.189, p = 0.047$). It seems that those who say they would feel more powerful while using a password manager are more likely to say they did not have a need for one in their comment. When considering that only 8% of comments mention both a security concern and a lack of need, this suggests that many of those who say they do not have a need still see some benefits in using a password manager since they generally rate that they would feel powerful while using one. On the other hand, those who say they have a lack of time/motivation in their comment generally rate feelings of power as lower, if they were to use a password manager. Like with grateful, this could reflect that, if they *had* to use a password manager, those who say they do not have time/motivation would feel *powerless* due to having further budget, in their words, limited time.

Next, to further understand the role of emotion on the decision to use or not use a password manager, we investigated differences in emotions between "users" and "non-users" of password managers. We performed Mann–Whitney U tests to evaluate the differences in emotion ratings between the two groups. We found significant differences in four emotions. Table 6 shows average and median response ratings for each group along with the resulting *U* statistic and significance value for U tests. The emotions secure, suspicious, admiring, and energetic received significantly different ratings from "users" and "non-users," suggesting that participants who use a password manager are more likely to feel secure, admiring and energetic, and less likely to feel suspicious. These results

Table 6 Participants were asked to agree on a scale of 1 = "Never" to 5 = "All the time" how they might feel each emotion while using password manager

Statement	Users	Non-users	U test	
	Mean (med.)	Mean (med.)	*U*	Sig.
Secure	3.80 (4)	3.50 (4)	6148	0.01
Energetic	2.58 (3)	2.21 (2)	6111	0.01
Admiring	2.66 (3)	2.32 (2)	6305	0.017
Suspicious	2.39 (2)	2.80 (3)	5788	0.01

Average and median response rating for each group are shown along with the resulting statistic comparing responses for given emotions

support our other finding that many of those who do not use password manager report doing so because they see password managers as insecure.

Discussion

We are not the first work to investigate the usability and user opinions of password managers. To better explain our findings and put them in context, we will discuss our results in more detail and explain how our findings compare with prior, related studies.

First, we found that "users" of password manager are more likely to have higher computer proficiency, and have generally better opinions/experiences with computer security and password managers. "Users" of password manager also generally find password managers to be more useful and convenient. On the other hand, "non-users" of password managers are more likely to rate their computer proficiency lower, report having fewer accounts, and use them less frequently. "Non-users" also generally think that they could be doing more to protect their accounts, but they do not see password managers as an effective way to do this. More "users" than "non-users" in our sample report higher technical expertise, especially in the area of computer security, which could reflect an actual higher technical proficiency among "users," as suggested by Ion et al. [8], which reported that experts are more likely to use password managers than non-experts.

From the qualitative comments, we found that convenience is important to many "users," but security concern is one of the main reasons why many "non-users" do not use a password manager. We argue that this divergence in opinion about security, combined with the quantitative findings suggest that many "non-users" do not see password managers as secure, which is not true for some applications, if used properly (e.g., LastPass). The primacy of convenience as a reason for using a password manager from "users" also suggests that some number, possibly many who use a password manager may not be aware of the security benefits. This could possibly stem from the misunderstanding of the tool, as noted by Chiasson and Karole [12, 13]. This trend is not limited to password managers. As Howe et al. saw in their 2012 literature survey of works about psychology in computer security in general, the desire to be secure, but a lack of understanding of the threats, solutions, and tools was found by many previous studies [25].

However, our study goes one step further and identified that even a large group of users of the tool do not completely understand the security benefit and use it primarily for convenience. In fact, multiple users of the tool reported that they do not trust the tool for their sensitive accounts, which should come as a warning to any who look to these results as motivation to focus too heavily on using convenience to encourage password manager use. Stobert and Biddle [29], when exploring users' coping strategies for password management (i.e., how they manage and keep track of their passwords), found that most users ration their efforts to protect accounts they feel are more important and minimize their efforts (e.g., by reusing password) for accounts of lesser importance. It is clear that, though promoting password managers based on their convenience may reap gains in overall adoption, a lack of trust in the tool and its security can still lead to "insecure" behavior by users because they will, as Stobert and Biddle suggest, avoid using password managers for sensitive accounts, somewhat defeating the security of using the tool.

Measurements for the 45 emotions were taken using self-reported ratings for each emotion that "users" say they feel and "non-users" say they would feel while using a password manager. Though this and their studies differ in methods and focus, we argue the findings in this paper somewhat support Kay and Loverock's [28] result that as knowledge increased, happiness increased while anxiety decreased with new software in that, in our study, several emotions for each group were correlated with computer proficiency. Though the emotions that correlated were different between the studies, deeper analysis of our data suggested that our correlation could be due to better knowledge of the tool's security benefits. Not only does this line up with prior studies, but this result also echoes our other findings related to the importance of technical expertise. Additionally, we found that several emotions were rated significantly different between the two groups, while most were not. These differences also suggest a difference in opinion regarding the security of the tool between the groups. Again, thinking to Kay and Loverock's findings and our finding of significant differences in computer proficiency between the groups, this could be due to lower knowledge about password managers or software in general. Overall, these findings show the importance of trust in and comfort with the security of the tool and software in general can play in people's decisions, whether already held by a user or gained through new knowledge/education. Considering the history of this notion in the literature and its prevalence in other analysis for this paper, it is clear that more needs to be done to increase the security awareness of password managers on a very fundamental level.

Finally, throughout this analysis, we have assumed that password managers are secure due to their common recommendation from experts, but what if those who distrust password managers in our study and elsewhere are right? Some recent work suggests that password managers may be insecure in some ways, calling for a more thorough look at the security of these tools [34]. Results like this and arguments from some that those who act "insecurely" are actually making perfectly rational and logical choices given their knowledge and experiences [15, 16] show that hearing both sides of the argument (i.e., to use and not to use) can be invaluable towards understanding not only what users are thinking, but also what they face. Our study finds that even many users do not necessarily see password managers as secure. When considering password managers' reputation as a convenience-oriented tool, that has documented vulnerabilities [34] (i.e., single point of failure), "non-users'" decisions begin to look more and more rational. Addressing real and imagined issues with the tool, partly through persuasive campaigns and user education should make strides towards increasing adoption of password managers.

Conclusion

In this paper, we presented the results of an online survey aimed at gaining insight into why some users choose to use or not use password managers. We identified that, while "users" of password manager noted convenience and usefulness as the main factors for using a password manager, "non-users" noted security issues as the chief reason for not using a password manager. This highlights that the purpose of such tools are often misunderstood by both "users" and "non-users." Analysis of differences in emotions between "users" and "non-users" of password managers reveals that participants who use a password manager are more likely to feel secure, admiring and energetic, and less likely to

feel suspicious when using their password manager to log into a website. These findings suggest that any effort which attempts to persuade users to adopt password managers will need to clearly explain the purpose of the tool and the technology behind it.

While prior research identified usability and security problems of existing password managers [12, 13, 34], they have not investigated the decision making process for those using or not using password managers, differences in opinions of each group, and emotional aspects of the decision. Therefore, we provide insights into why some users choose to use password managers while others choose not to, and identify that the purpose of password managers are often misunderstood by both "users" and "non-users," indicating a widespread problem of miscommunication for the security tool.

Authors' contributions
YA and MF designed the study and prepared the necessary materials under the supervision of MK other than the emotion portion of the survey, which was developed by RB. YA and MF conducted the study under the supervision of MK. YA and MF analyzed the collected data. YA, MF and MK developed the final code plan which then used to develop the final coding of the responses presented. YA, MF and MK drafted and edited the report. All authors read and approved the final manuscript.

Author details
[1] Department of Computer Science and Engineering, University of Connecticut, Storrs, CT, USA. [2] Department of Communication, University of Connecticut, Storrs, CT, USA.

Competing interests
The authors declare that they have no competing interests.

Funding
This work is supported by the National Science Foundation under Grant No. CNS-1251962 and CNS-1343766, and GAANN Fellowship No. P200A130153. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agency.

Appendix

Survey questions

This final portion presents the survey questions used in the password manager survey. Some of the questions used in our study were adopted from prior work and modified accordingly.

- What is your gender?
  - ○ Male
  - ○ Female
  - ○ Other
- What is your age?
  - ○ 18-25
  - ○ 26-34
  - ○ 35-54
  - ○ 55-64
  - ○ 65+
- What is the highest level of education you have received?
  - ○ Less than High School
  - ○ High School / GED
  - ○ Some College
  - ○ 2-year College Degree
  - ○ 4-year College Degree
  - ○ Master's Degree
  - ○ Doctoral Degree
  - ○ Professional/Medical Degree (JD, MD)
- What is your level of computer proficiency?
  - ○ Very low
  - ○ Low
  - ○ Below average
  - ○ Average
  - ○ Above average
  - ○ High
  - ○ Very high
- How often do you go online?
  - ○ Never
  - ○ Less than once a month
  - ○ 1-3 times a month
  - ○ Once a week
  - ○ 2-3 times a week
  - ○ 4-5 times a week
  - ○ More than 5 times a week
- To your knowledge, have you ever had an account hacked or compromised by attackers?
  - ○ Yes
  - ○ No
- How many accounts for Internet websites and services do you have in total?
  - ○ None
  - ○ 5 or less
  - ○ 10 or less
  - ○ 20 or less
  - ○ 50 or less
  - ○ more than 50
  - ○ More than 5 times a week
- On an average week, how many of those accounts do you use?
  - ○ None
  - ○ 5 or less
  - ○ 10 or less
  - ○ 20 or less
  - ○ 50 or less
  - ○ more than 50
- How many unique passwords do you have in total?
  - ○ One I use the same password for all accounts
  - ○ Few I use more than one, but not many different passwords on different accounts
  - ○ Several I use multiple passwords across multiple accounts, but sometimes reuse
  - ○ Many I use a different password for every account, I don't reuse any password
  - ○ 50 or less
- Do you know what a password manager is?
  - ○ Yes
  - ○ No
- Have you ever used a password manager?
  - ○ Yes
  - ○ No

Tables 7, 8 and 9 show all the statements used in the survey. For all statements in Tables 7 and 8, participants were asked to rate how much they agree with each statement from 1 = Strongly disagree to 5 = Strongly agree. For statements in Table 9, they were asked how much they might feel each emotion from 1 = Never to 5 = All of the time.

Table 7 Statements that were shown to both "users" and "non-users" in a grid format. Most of the statement in this table were adopted from [30], and modified accordingly

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I am doing a good job of protecting my computer security	◯	◯	◯	◯	◯
I could do more to protect my accounts	◯	◯	◯	◯	◯
I do not have time to pay attention to security	◯	◯	◯	◯	◯
I do not feel that my accounts are likely to be attacked	◯	◯	◯	◯	◯
I do not know where to get computer security advice	◯	◯	◯	◯	◯
I am knowledgeable about computer security	◯	◯	◯	◯	◯
I care about computer security	◯	◯	◯	◯	◯
I trust my computer	◯	◯	◯	◯	◯
I am worried about the security of some of my account/devices more than others.	◯	◯	◯	◯	◯
Passwords are easy to remember	◯	◯	◯	◯	◯

Table 8 Statements that were shown to both "users" and "non-users" in a grid format. Most of the statement in this table were adopted from [30], and modified accordingly

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I trust password managers	◯	◯	◯	◯	◯
Password managers are more secure	◯	◯	◯	◯	◯
Password managers help people	◯	◯	◯	◯	◯
Password managers are easy to use	◯	◯	◯	◯	◯
Password managers are more convenient	◯	◯	◯	◯	◯
I understand the theory behind password managers	◯	◯	◯	◯	◯
I understand why password managers are secure	◯	◯	◯	◯	◯
I worry that accessing my accounts may be more difficult with a password manager	◯	◯	◯	◯	◯

Table 9 Emotions that were rated by participants

Emotions
1. Confident (e.g., because one is protected from possible danger)
2. Secure (e.g., because one is protected from possible danger)
3. Sad (e.g., because one's time is being used by the password manager)
4. Depressed (e.g., because one's time is being used by the password manager)
5. Down (e.g., because one's time is being used by the password manager)
6. Afraid (e.g., because one's time is being used by the password manager)
7. Nervous (e.g., because one's time is being used by the password manager)
8. Anxious (e.g., because one's time is being used by the password manager)
9. Angry (e.g., because using the password manager is inconvenient)
10. Insulted (e.g., because using the password manager is inconvenient)
11. Hostile (e.g., because using the password manager is inconvenient)
12. Surprised (e.g., because one does not expect how hard or easy the password manager is to use)
13. Dazed (e.g., because one does not expect how hard or easy the password manager is to use)
14. Confused (e.g., because one does not expect how hard or easy the password manager is to use)
15. Freaked out (e.g., because one does not expect how hard or easy the password manager is to use)
16. Disgusted (e.g., because using the password manager is inconvenient)
17. Dismayed (e.g., because using the password manager is inconvenient)
18. Distraught (e.g., because using the password manager is inconvenient)
19. Cared-for (e.g., because one is protected from possible danger)
20. Friendly (e.g., because one is protected from possible danger)
21. Welcomed (e.g., because one is protected from possible danger)
22. Powerful (e.g., because one knows of danger and is taking precautions)
23. Energetic (e.g., because one knows of danger and is taking precautions)
24. Vigorous (e.g., because one knows of danger and is taking precautions)
25. Isolated (e.g., because one's precautions may be inadequate)
26. Lonely (e.g., because one's precautions may be inadequate)
27. Abandoned (e.g., because one's precautions may be inadequate)
28. Proud (e.g., because one knows of danger and is taking precautions)
29. Triumphant (e.g., because one knows of danger and is taking precautions)
30. Arrogant (e.g., because one knows of danger and is taking precautions)
31. Ashamed (e.g., because one's precautions may be inadequate)
32. Guilty (e.g., because one's precautions may be inadequate)
33. Embarrassed (e.g., because one's precautions may be inadequate)
34. Scornful (e.g., because the danger is easily countered)
35. Contemptuous (e.g., because one is protected from possible danger)
36. Disdainful (e.g., because one is protected from possible danger)
37. Humiliated (e.g., because one is protected from possible danger)
38. Dishonored (e.g., because one is protected from possible danger)
39. Resentful (e.g., because the danger is not easily countered)
40. Grateful (e.g. because the system has given one tools to respond)
41. Respectful (e.g. because the system has given one tools to respond)
42. Admiring (e.g. because the system has given one tools to respond)
43. Trusting (e.g. because the system has given one tools to respond)
44. Suspicious (e.g. because the tool may be unreliable)
45. Happy (e.g., because one is protected from possible danger)

The entries above were prefixed with "One might feel ..." to create the question used on the survey

Received: 17 March 2016 Accepted: 6 March 2017
Published online: 15 March 2017

References

1. Florencio D, Herley C (2007) A large-scale study of web password habits. In: Proceedings of the 16th international conference on World Wide Web. ACM, New York City, pp 657–666
2. Halderman JA, Waters B, Felten EW (2005) A convenient method for securely managing passwords. In: Proceedings of the 14th international conference on World Wide Web. ACM, New York City, pp 471–479
3. Cnet. take control of password chaos with these six password managers. http://www.cnet.com/news/best-password-managers/. Accessed 02 Sept 2016
4. Security of password managers. https://www.schneier.com/blog/archives/2014/09/security_of_pas.html. Accessed 02 Sept 2016
5. Wall street journal. the best way to manage all your passwords. http://www.wsj.com/articles/SB10001424052702303647204579545801399272852. Accessed 02 Sept 2016
6. Grosse E, Upadhyay M (2013) Authentication at scale. Secur Priv 11(1):15–22
7. Huth A, Orlando M, Pesante L (2012) Password security, protection, and management. United States Computer Emergency Readiness Team
8. Ion I, Reeder R, Consolvo S (2015) "... no one can hack my mind": cmparing expert and non-expert security practices. In: Symposium on usable privacy and security (SOUPS)
9. Buck R, Anderson E, Chaudhuri A, Ray I (2004) Emotion and reason in persuasion: applying the ari model and the CASC scale. J Bus Res 57(6):647–656
10. Das A, Bonneau J, Caesar M, Borisov N, Wang X (2014) The tangled web of password reuse. In: Symposium on network and distributed system security (NDSS)
11. Ives B, Walsh KR, Schneider H (2004) The domino effect of password reuse. Commun ACM 47(4):75–78
12. Chiasson S, van Oorschot PC, Biddle R (2006) A usability study and critique of two password managers. In: Proceedings of the 15th USENIX security symposium, Vancouver, Canada, August 2006
13. Karole A, Saxena N, Christin N (2011) A comparative usability evaluation of traditional password managers. In: Proceedings of the 13th international conference on information security and cryptology, ICISC'10. Springer, Berlin, pp 233–251
14. Fagan M, Khan MMH (2016) Why do they do what they do? A study of what motivates users to (not) follow computer security advice. In: Twelfth symposium on usable privacy and security (SOUPS 2016). USENIX Association, Berkeley, pp 59–75
15. Herley C (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 workshop. ACM, New York City, pp 133–144
16. Herley C (2014) More is not the answer. Secur Priv 1:14–19
17. Dunphy P, Vines J, Coles-Kemp L, Clarke R, Vlachokyriakos V, Wright P, McCarthy J, Olivier P (2014) Understanding the experience-centeredness of privacy and security technologies. In: Proceedings of the 2014 workshop on new security paradigms workshop. ACM, New York City, pp 83–94
18. Egelman S, Peer E (2015) The myth of the average user: improving privacy and security systems through individualization. In: Proceedings of the 2015 new security paradigms workshop. ACM, New York City, pp 16–28
19. Harbach M, Hettig M, Weber S, Smith M (2014) Using personal examples to improve risk communication for security & privacy decisions. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM, New York City, pp 2647–2656
20. Das S, Kim THJ, Dabbish LA, Hong JI (2014) The effect of social influence on security sensitivity. In: Tenth symposium on usable privacy and security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA, pp 143–157
21. Fagan M, Khan MMH, Buck R (2015a) A study of users' experiences and beliefs about software update messages. Comput Hum Behav 51:504–519
22. Fagan M, Khan MMH, Nguyen N (2015b) How does this message make you feel? A study of user perspectives on software update/warning message design. Hum Centric Comput Inf Sci 5(1):1–26
23. Vaniea KE, Rader E, Wash R (2014) Betrayed by updates: how negative experiences affect future security. In: Proceedings of the 32nd annual ACM conference on Human factors in computing systems. ACM, New York City, pp 2671–2674
24. Wash R, Rader EJ, Vaniea K, Rizor M (2014) Out of the loop: How automated software updates cause unintended security consequences. In: Tenth symposium on usable privacy and security (SOUPS)2014, July 9–11,2014, Menlo Park, CA, pp 89–104
25. Howe AE, Ray I, Roberts M, Urbanska M, Byrne Z (2012) The psychology of security for the home computer user. In: 2012 IEEE symposium on security and privacy (SP). IEEE, New York, pp 209–223
26. Ferrer RA, Fisher JD, Buck R, Amico KR (2011) Pilot test of an emotional education intervention component for sexual risk reduction. Health Psychol 30(5):656
27. Bagozzi RP, Pieters R (1998) Goal-directed emotions. Cognit Emot 12(1):1–26
28. Kay RH, Loverock S (2008) Assessing emotions related to learning new software: the computer emotion scale. Comput Hum Behav 24(4):1605–1623
29. Stobert E, Biddle R (2014) The password life cycle: user behaviour in managing passwords. In: Symposium on usable privacy and security (SOUPS 2014). pp 243–255
30. Stobert EA (2015) Graphical passwords and practical password management. Ph.D. thesis, Carleton University Ottawa, Ottawa
31. Zar JH (1972) Significance testing of the spearman rank correlation coefficient. J Am Stat Assoc 67(339):578–580
32. Field A (2013) Discovering statistics using IBM SPSS statistics, 4th edn. Sage Publications Ltd., Los Angeles
33. Miles MB, Huberman AM (1994) Qualitative data analysis: an expanded sourcebook. Sage, London
34. Li Z, He W, Akhawe D, Song D (2014) The emperor's new password manager: security analysis of web-based password managers. In: 23rd USENIX security symposium (USENIX Security 14). USENIX Association, Berkeley