So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?

Sal Aurigemma
University of Tulsa
sal@utulsa.edu

Tom Mattson
University of Richmond
tmattson@richmond.edu

Lori Leonard
University of Tulsa
lori-leonard@utulsa.edu

Abstract

In this paper, we investigate the voluntary use of password management applications in order to address a decades-old and ubiquitous information security problem related to poor password management. In our exploratory analysis, we investigate two related issues: (1) why home end-users chose not to use password management applications and (2) why high behavioral intentions to use password management applications did not always lead to actual usage for certain users. We found that issues related to the technology such as lack of trust or memory limitations, individual issues such as perceived costs and benefits, and a lack of concern about the threat (threat apathy) were the primary inhibitors of lack of use. For those that had high intentions to use a password management application but failed to actually use the software, we found that a variety of individual issues such as lack of immediacy and having insufficient time were the primary inhibitors leading to this breakdown.

1. Introduction

Organizations often rely upon tailored information security policies (ISPs) and security education training and awareness (SETA) programs to inform employees of the security threats they face and the appropriate, and often mandatory, actions to mitigate those threats [10, 12]. Improving the content and impact of corporate SETA programs is often a goal of organizational security behavior research [29, 18]. Home end-users, in comparison, do not have the benefit of an established ISP or professional SETA program in their personal lives [2]. As a result, home end-users may have little understanding of the security threats they face or the tools and actions they can take to protect their information assets [2].

Even if home end-users do understand the risks and appropriate mitigating actions, prescriptive security behaviors are completely voluntary. For example, although users may understand the need to keep their PC's operating system current with the latest security updates, compliance is completely voluntary with few repercussions until a security incident, such as a ransomware or malware infection, occurs. Research into improving home end-user security behaviors is thus challenged by a potential lack of threat awareness, lack of awareness of mitigating security behaviors, and perhaps even a lack of desire to voluntarily take recommended actions [2].

One home end-user information security behavior related to a variety of different threats is password management. Within organizations, employers typically mandate the use of strong passwords and the regular changing of those passwords. However, home end-users do not have this mandate and often do not change their relatively weak passwords [21]. Due to the difficulty in maintaining and remembering multiple passwords, many home end-users also have a single password for multiple sites, which is very problematic especially if the password is relatively weak [13, 38].

Password management applications exist to help resolve these types of problems, especially for the home end-user who does not benefit from built-in network applications that require certain types of password practices. Computer security professionals, the United States Computer Emergency Readiness Team (US-CERT), and the internationally recognized SANS Institute all strongly recommend the use of password manager applications [45, 25, 26]. Yet, adoption rates in the workplace and for home end-users are very low [24]. The purpose of our paper is to investigate why this is the case. We specifically address the following two interconnected research questions: (1) why do home end-users fail to adopt password management applications and (2) why do certain home end-users have high behavioral intentions to use password management applications but then fail to follow through on those intentions?

In order to address these research questions, we conducted an empirical investigation of 283 college

URI: http://hdl.handle.net/10125/41650
ISBN: 978-0-9981331-0-2

students who were presented information about the risks of poor password management and given the recommendation to adopt the use of a dedicated password manager application. The participants decided to either voluntarily adopt (or not) the use of a free commercial password management application. We then asked our research subjects open ended questions concerning their adoption intentions and the reasons why they actually adopted and used the password management application. We found individual issues related to laziness, lack of time, and lack of immediacy were the primary behavioral inhibitors, while the strongest behavioral enabler was a belief in the response efficacy of the recommended password management application. We also found a variety of individual issues led to the breakdown between having high behavioral intentions to use the software and a failure to actually use the software.

2. Background & Related Literature

Much of the research on information security practices focuses on behavioral intentions and not on actual behaviors [41, 14]. This is primarily due to decades of research that has empirically demonstrated that there is *generally* a fairly strong correlation between behavioral intentions and actual behaviors across a variety of actions [1, 3, 22]. However, more recent studies have started to evaluate both security intent and actual behaviors [15, 44, 7], but none have specifically explored factors that inhibit or support the transition from intent to actual behavior.

Numerous theories have been used to explain behavioral intentions in the context of information security actions. The most common theoretical perspectives are the theory of planned behavior, protection motivation theory, and general deterrence theory [4]. Most of the published research, irrespective of the theories being used, focuses on the first or second order antecedents of behavioral intentions with the assumption that there is a strong link between intentions and actual behaviors. This has largely been left as an untested assumption. Therefore, more research is needed to determine the enablers and inhibitors associated with the link between security related behavioral intentions and actual behaviors [41, 14].

In addition to suggesting that future information security research focus on both behavioral intentions and actual behaviors, Siponen and Vance [36] call for information security research that has more practical value in the user context. One such practically relevant security issue, but still theoretically rich, is password management. The password is still the primary means of protecting personal information online [25] and managing (which includes remembering) all of one's different passwords is still a major problem [42], especially for home end-users who tend to be very casual concerning their passwords [21].

The primary problems associated with end-user passwords is that they are often weak (easy to guess) and many users re-use the same password on multiple online accounts [25, 45]. Whereas weak passwords will always be easy for criminals to guess, even the use of very strong passwords on multiple accounts is dangerous because all it takes is one account to be compromised for several other accounts to be affected. Survey data indicate that up to 2/3 of online users use the same password for multiple or all online accounts [17, 30].

The effect of poor password management practices is tangible. According to the well-respected 2016 Verizon Data Breach Investigations Report (DBIR), legitimate user credentials (login ids and passwords) were used in over 50% of all reported data breaches in 2015. An analysis of 2260 confirmed data breaches in 2015 determined 63% involved "leveraging a weak, default, or stolen password" [40] (p. 20). Separate analysis of actual attacker tactics shows they specifically target end-user passwords in order to gain access to both personal and corporate information resources [6].

The security actions recommended to combat weak and/or reused passwords are to create and use only strong passwords and use a unique password for each end-user account [35]. Strong passwords are typically defined as passwords that contain at least 12 alphanumeric characters, both upper and lower case letters, at least one number, and at least one special character [35]. Unfortunately, the average end-user has dozens of personal and work-related passwords [17], and remembering many strong passwords is difficult. To assist users with proper password hygiene, the use of password manager applications is strongly recommended [45, 25]. Password management applications store all of a user's passwords in one location that is cryptographically protected and accessible through one (ideally) strong master passphrase, alleviating the burden of memorizing many unique strong passwords [25]. Empirical analysis of actual password behaviors has shown that users can remember a small number of strong, complex passwords, especially when used often (such as when unlocking the password manager) [42].

There are many password managers available for purchase, including several highly-regarded free applications. In this study, we introduced the

participants to several password managers but specifically recommended the use of LastPass, a free password manager that is widely used in both enterprises and by end-users (see https://lastpass.com/ for more detail).

From the behavioral adoption perspective, there are two main issues associated with password management applications that require additional research. First, behavioral intentions to use password management software have been shown to not be good indicators of actual usage of the software [42]. This makes password management applications an excellent context to investigate the link between intention to use the software and actual use of the software, which will strengthen the theoretical understanding of security adoption technologies (more broadly than just password management applications). For instance, it is possible that certain antecedents of intentions may be better contextualized as both direct and indirect effects on actual behaviors.

Second, adoption rates of password managers are very low [24, 26]. This category of software solves a very important problem, but home end-users have low adoption intentions and actual usage of these software packages [33, 26]. Therefore, it is important from both a theoretical and a practical standpoint to understand why this is the case. Existing literature offers certain hypotheses such as the software may be difficult to use, the real or perceived costs of using these applications may outweigh the benefits, a lack of self-confidence on behalf of the home end-user, and so on [4]. More research is needed to further our understanding of the low adoption rates of a category of applications that is, generally speaking, highly useful and purportedly easy to use.

3. Research Design & Methods

3.1 Research Subjects

In order to investigate password management software adoption among home end-users, we used undergraduate college students from a US private university as our research subjects. While there is often criticism about using college students in academic research, much of that criticism comes from trying to extend the results of student-derived data to other organizational contexts and populations [31]. When investigating home end-user information security practices, however, we consider college students an excellent population to study due to their extensive use of technology, familiarity with online applications (such as social networking sites and school-related information systems), and also the perception that college students are not overly conscientious with their information privacy and security [20, 23]. Additionally, many college students are expected to enter the greater work force in the next 1 to 4 years. Therefore, understanding and improving the security behaviors of this demographic is important at both the individual and organizational levels. Furthermore, numerous studies that have explored security behaviors (including password management) [7, 38, 42, 16, 27] have used college students in their research studies.

A total of 372 undergraduate students were provided the opportunity to participate in this study in return for a small amount of course extra credit. A total of 286 responses were collected during the first phase of the data collection (which included the fear appeal and measurement of behavioral intent), representing a 77% response rate. After eliminating those who participated in the first part of the study but did not complete the second phase (which collected information about actual security behavior), we were left with 283 usable data points for the second phase.

Of the 283 usable data points, 10 (3.5%) were already using a dedicated password manager application (LastPass 1Password, KeePass, or similar). These 10 participants were asked more detailed questions about their experiences with password management software and excluded from the second phase of our study. From the remaining 273 participants, 37 (13.5%) decided to install and use a password manager after the first data collection phase, and 236 (86.5%) decided not to install and use the application.

3.2 Data Collection

The first phase of the data collection provided the participants with a link to an online video that included a fear appeal message related to poor password management and a survey to measure behavioral constructs and their intent to install and use a password manager within the following week. The fear appeal inside of the threat message is crucial in defining the threat and providing mitigating actions [7, 27]. For this part of our study, we used the guidelines of Witte, et al. [43] and the summarized fear appeal findings from Ruiter, et al. [34] to build our fear appeal message. Witte, et al. [43] argue that successful fear appeals must include two components – (1) a threat component that articulates the magnitude of the threat whereby there is a real possibility that the danger associated with the threat can occur to the participant (on a personal level), and (2) a recommended response that communicates that the prescriptive solution works, is within the capability of the recipient of the message, and also addresses common barriers from performing the

designated response. The specific threat message was formatted in a video (available at https://www.youtube.com/watch?v=ru3JXo7YoVc). The contents and video format of the message were developed through a series of three pilot studies with students and academics.

All questions for the survey instrument came from pre-existing and pre-validated scales. From Boss, et al. [7], we used the definition of behavioral intent as the self-reported intention to perform the subject security action (in this case, install and use a password manager). Behavioral intent to use a password manager application was measured in both data collection phases (immediately after the security threat message and one week later when actual behavior was measured). In order to differentiate between whether a participant merely downloaded the recommended software or actually used the application to perform password management functions, we asked several questions that could be answered only by using the "Security Challenge" tool built into the password manager. These questions included the users providing the relative strength of their master password associated with their password manager, the aggregate security score for all their accounts as determined by the application, and the total number of accounts in their password manager application at the time of data collection. These additional details were captured to provide proof of application installation *and* use that could only come from a password manager and also to gather data about initial use of the password manager application for areas of future examination.

The second phase of the data collection was conducted one week after completion of the first survey to ascertain whether the participants followed through with the security behavior, which was the adoption of the password management application. The timeframe of one week between data collection was determined by interviewing 15 students who were taking part in a class-related password manager application pilot study. These students almost unanimously stated that if they did not take a voluntary action within a couple of days of being exposed to the action, they would probably never take the recommended action without being re-prompted. One week was chosen to conservatively allow enough time for a participant to voluntarily install a password manager application or not.

In the second phase of the data collection, participants were asked whether they took the recommended, yet voluntary, security-relation action to download and start using a free password manager application (LastPass) or some other password manager. Actual behavior was adjudicated based upon questions that could only be answered through the use of a password manager (as described above). Participants that chose *not* to use a password manager were asked an open-ended question about the reasons they used to justify the non-action as well as their intentions to use a password manager sometime in the future.

3.3 Qualitative Analysis

Empirical analyses of participant responses focused on identifying and exploring behavioral factors that interfered with or facilitated the transition of intending to install and use a password manager. To accomplish this goal, we conducted an iterative coding process modeled after Vaast and Kaganer [39].

The first step of the analyses consisted of inductive open coding [39] of the participant open-ended responses for both compliance with the recommended security behavior (use of a password manager) and non-compliance. We started by having two of the authors randomly select 50 participant responses from the dataset and code them independently. There was no *a priori* coding schema; we allowed the codes to emerge from the data. A coding unit was defined as a segment of text ranging from one sentence to one paragraph. However, a single segment of text could include several codes.

We coded the 50 responses independently from each other. After each of the coding rounds, we reviewed our respective codes and reconciled any discrepancies through discussion prior to consolidating the findings. Per [39], we used the coding schema from the first round to evaluate another 50 randomly-selected responses each, while simultaneously modifying and extending the coding schema to capture new and emerging themes and concepts [19].

In order to ensure that all coders understood the definitions of each category, we brought in another coder that did not take part in the code creation process. One of the original coders and the new coder examined 50 responses together using the final coding schema and then independently coded a sample of the same 100 responses to assess inter-rater reliability. The two coders agreed 89% of the time, which is a simple Cohen's Kappa value of 0.85, suggesting an acceptable level of inter-coder reliability [28]. Coding disagreements were discussed and resolved together. Eventually, we evaluated all of the responses iteratively and independently. The resulting coding scheme and associated themes are defined and illustrated with examples in Table 1.

4. Results

Although the focus of this paper is on qualitative content analysis, we do incorporate basic descriptive statistics in order to further guide the interpretation of our data, which is consistent with the recommendation of Boyatzis [9]. The behavioral intentions scores of those that chose not to take the security action (mean = 4.05, n = 236, s.d. = 1.43) showed effectively neutral intentions to install and use a password manager, which played out. However, comparing the results of the first phase behavioral intentions scores with the second phase data collection scores for these participants (mean = 4.66, n = 236, s.d. = 1.48) showed a statistically significant increase in the same population's intention to use a password manager in the future ($t = -7.02$, $df = 237$, $p < 0.001$). This indicates that study participants that were exposed to the poor password management threat message from this study were influenced to at least consider using a password manager in the future following the second phase of the data collection. We did not measure whether this same group of participants eventually did install and use a password manager.

Our qualitative data analysis identified eight individual behavioral inhibitors that influenced study participants against taking the recommended security action of installing and using a dedicated password manager application. We grouped these factors into three main themes: (1) Individual Inhibitors, (2) Threat Apathy, and (3) Technology Inhibitors.

4.1 Individual Inhibitors

We define individual inhibitors as any real or perceived conflict with or drain on limited individual resources to include tangible assets (such as time and money) or cognitive capacity (such as memory, perceived self-efficacy, expected effort required). Individual inhibitors were reported by 72% of the study participants. Our analysis identified four factors (presented in order of highest occurrence) that interfered with our participants' personal capacity to take the recommended security action.

Insufficient Time

The most common factor cited in our study (41% of the participants) for deciding not to take the recommended security action was a perceived lack of time to install (or configure) and use the password manager. In many cases, the respondents explicitly stated an intention to take the security action, but other tasks had higher priority. For example:

> "I thought about installing a password manager application, but just didn't have the time to set aside to do so."

In some extreme cases, the respondents took a cavalier approach towards their lack of time management, identifying themselves as lazy even in the face of danger.

> "Most likely arrogance and being lazy. I have never had one of my passwords stolen so would most likely wait until that happened before installing a password manager."

Lack of Immediacy

A sizable portion (15%) of the participants identified their intent to take the security action, but because they did not act promptly, they ended up forgetting to do so. This is an interesting issue, especially with all of the distractions from the plethora of different gadgets that users face on a daily basis. For example,

> "I got distracted by something else and honestly forgot, but when I remember I want to try one!!"

And, in numerous cases, having to identify the main reason for their inaction led to a restatement of their planned intent to take the security action in the future (which is supported by the quantitative analysis reported earlier).

> "I forgot about it--I will install one now that I've been reminded again."

Excessive Effort Required

The third most cited (12.2% of respondents) individual behavioral inhibitor related to the perceived effort required to take the security action. When the expected effort required to install and populate the password manager was perceived as more than the participant was willing to expend to counter the password management threat, they abandoned their intentions to take the action.

> "I didn't want to take the time to set up a new application and enter in all my passwords."

However, there were cases where the expected level of effort would be considered acceptable in the future when the participants' professional circumstances changed.

Table 1: Themes, codes, definitions, and examples from participants that did not perform the recommended security action

Theme	Codes (Behavioral Inhibitors)	Definitions	Examples
Individual Inhibitors (Salience = 72%)	Insufficient Time	Participants reported that they did not have the slack time resources to allocated towards taking the security action	"Time. I put it on my todo list but I prioritized other things. To be fair, i'm usually slow about doing updates and such. I will do it eventually."
	Lack of Immediacy	Participant planned to install the application but did not so do promptly; in time they eventually forgot to follow through with their intention.	"I honestly forgot, but when I remember I want to try one!! "
	Excessive Effort	Expected effort to install and populate the password manager is more than the participant wants to expend	"I didn't want to take the time to look up my password every time I encountered a log in. It would be time consuming for something that I do not feel I am at high risk for."
	Low Self-efficacy	Participants unsure if they are capable of installing and using password manager applications properly	"I feel as though I am not good enough with computers to know how to install a password manager so I'll just try to remember my passwords."
Threat Apathy (Salience = 25%)	Threat Apathy	Participants do not think that the threats from poor password management are worthy of taking any additional action.	"I do not feel like I need one. I typically remember most of my passwords even if it takes me a try or two for a site I do not have to enter the password for very often."
Technology Inhibitors (Salience = 20%)	Alternative Solution	Participants already have some kind of password management system in place, but not a dedicated application.	"I feel that I can more effectively manage my own passwords by manually recording them in a physical notebook."
	Lack of Trust	Participants do not trust password manager applications to keep their passwords safe	"Not super interested, and keeping all of my passwords in one place scares me.
	Insufficient Awareness	Participant requires additional information about password managers before deciding to take the security action	"I am still thinking about it, I want to understand how to use it and install it."

"I didn't think it would be very useful at this point in my life. I'm about to graduate and get all new emails and accounts so maybe in the future when I'm all settled in my full time job it will be more beneficial and worth the effort to get a password manager application."

Low Self-efficacy

The final individual inhibitor (5% of participants) related to the participants' self-assessed ability to successfully complete the recommended security action. Self-efficacy, a central tenet of social cognitive theory and the theory of planned behavior, represents an individual's belief that they are capable of performing a specific behavior where higher self-efficacy results in greater effort to persist in the face of obstacles [5]. A small group of participants identified low self-efficacy with computer technology as the primary reason they did not take the security action.

"I feel as though I am not good enough with computers to know how to install a password manager so I'll just try to remember my passwords."

Others felt that perhaps the installation and use of the password manager application itself was beyond their capabilities.

"To add the password manager application onto my computer seems simple enough, but getting all the information in it and then using it seems a little bit too complex. I will try the password manager application after final exams when I am able to get some help from my techie friend."

4.2 Threat Apathy

The second most common theme or category of behavior inhibitors was threat apathy. Threat apathy occurs when individuals do not necessarily pay attention to security because they just do not consider the recommended information security action (and its related threat) to be important [8, 37]. Exactly one quarter (25%) of respondents felt that the threat of poor password management was not a big enough concern for them to change their current security behaviors.

"Although the survey made me more wary against cyber security faults, I still don't feel it necessary to have a password manager app."

In many cases, the participants felt that their status-quo behaviors were sufficient for the threat, regardless of the evidence about the consequences of poor password management.

"I do not feel like I need one. I typically remember most of my passwords even if it takes me a try or two for a site so I do not have to enter the password very often."

In some extreme cases (2% of the sample population), participant hubris of their current password management skills and memory (without a password manager) exacerbated their threat apathy to a feeling of invulnerability.

"I did not find my personal information to be in danger because there is absolutely no way anyone can guess my passwords but I can remember them."

4.3 Technology Inhibitors

The final category of behavioral inhibitors (reported by 20% of the participants) pertained to password manager application technology itself. Our analysis identified three factors (presented in order of highest occurrence) about password manager application technology that represented the main reasons for not installing and using one.

Insufficient Awareness

Some participants (10%) reported that they were interested in taking the recommended security action but required more information about how to install and use the actual tool in order to decide on moving forward with the password manager application. This awareness deficiency represents an explicit knowledge gap in the participants' understanding of how the technology works and/or how to install and use it, as opposed to a perceived lack of ability to do so (low self-efficacy).

"I have not researched and found a good one to use yet."

One solution to their awareness deficiency, beyond researching password managers themselves, was for some participants to reach out to friends and family for additional information and guidance on using password managers.

"I have not asked some of the people I trust (my dad and his work friends) if they use password managers."

A small group (2%) of participants reported concern about the amount of space the password manager application would take up on their electronic devices.

"I am not sure which one to use and where to download it, and I am not sure how much space it will take up on my computer."

Alternative Solution

A small group of participants (7%) reported that they were satisfied with their current password management

system. The alternative solutions included relying on personal memory for all passwords, writing the passwords down in a physical notebook, and use of built-in computer password managers (web browser password storage, iCloud keychain, etc).

Lack of Trust

The final behavioral inhibitor related to the technology is a lack of trust (5% of respondents) that password managers will keep their information safe. The main concerns were having all the passwords in one location

> "Not super interested, and keeping all of my passwords in one place scares me."

> And storing the password bank on the Internet.
> "I don't want my passwords online in one place."

4.4 Inhibitors of High Behavioral Intent Participants

The behavioral inhibitors identified in sections 5.1 through 5.3 emerged from the analyses of all participants' responses in the sample and address the first research question of why do home end-users fail to adopt password management applications. In order to address the second research question of why certain home end-users have high behavioral intentions but then fail to follow through on those intentions, we isolated the coded responses for all participants that showed a positive inclination (intention) towards taking the security action (by selecting average behavioral intent scores of 5 or greater on a 7 point Likert scale as discussed in Section 3.2). Table 2 shows the ranked (in order of occurrence) behavioral inhibitors for both the entire sample and just the 59 participants that met the positive intention criteria.

As seen on Table 2, those with higher behavioral intention scores were not inhibited by trust or low-self efficacy issues. Additionally, while the perceived lack of time to install and use a password manager was still the primary inhibitor between intent and actual behavior, the order of precedence for the remaining behavioral inhibitors differs noticeably between the two groups. For example, the high-intention group showed a relative decrease in the importance of threat apathy as compared to the group as a whole. While the number of subjects in the high-intent group is relatively small (n=59), the results as shown in Table 2 suggest that addressing behavioral inhibitors with this group requires a different focus of effort in future threat messages and security awareness campaigns compared to users with lower intent scores.

Table 2: Group comparison of behavioral inhibitors

Codes (Behavioral Inhibitors)	High Behavioral Intent Group		Whole Sample	
	Relative Ranking	Occurences (n=59)	Relative Ranking	Occurences (n=236)
Insufficient Time	1	35	1	97
Lack of Immediacy	2	8	3	35
Insufficient Awareness	3	7	5	19
Threat Apathy	4	6	2	59
Alternative Solution	5	5	6	16
Excessive Effort	6	3	4	29
Lack of Trust	N/A	0	7	12
Low Self-efficacy	N/A	0	8	10

5. Discussion and Future Research

The main purpose of this study was to investigate why home end-users adopt or fail to adopt (both intentions and actual adoption) password management applications. On the surface, these applications significantly reduce the risks associated with poor password management and are, by all reported accounts, very easy to use. Yet, adoption rates among home end-users is very low [24]. Through our analyses, we identified three predominant categorical themes consisting of eight individual behavioral inhibitors. Individual factors such as lack of immediacy and perceived lack of time were the most common reasons why our study participants identified as not downloading and using a password management application.

Interestingly, a large portion of our subjects were quite naïve in terms of the threat associated with poor password management, which we labeled as threat apathy. Even after seeing a password threat video outlining the threat and its associated dangers, the majority of subjects still did not recognize this as an issue that needed solving, which is quite troubling given the statistics related to poor password management among home end-users. As a result, it is not surprising that having a high level of threat apathy resulted in very low adoption rates. Our subjects did identify technology related issues inhibiting their adoption, but this was the least important of our identified themes. This may be the case, because most of these applications are very easy to use (e.g., simplicity in use but complex in design) and other factors besides the software were driving the adopt versus not adopt decision.

Several of the identified behavioral inhibitors have been explored in some fashion in previous security behavior-related research, but that research was primarily focused on better understanding the antecedents of security behavioral intentions. For example, Bulgurcu, et al. [11] developed and tested a security behavior model that measured the effects of self-efficacy, response-efficacy, and rational choice perceived compliance costs on user attitudes toward an intentions to follow general security policies by

organizational employees. Likewise, Boss, et al. [8] found that threat apathy was a deterrent to employee intent to follow organizational security policies. What makes our study unique is that we identified these factors as potential inhibitors that affect the transition between intent and actual behavior.

We intend to take the findings of this research to improve the threat message about poor password management by specifically addressing the key behavioral inhibitors identified in the present study with the goal of increasing the rate of successful security behavior beyond the 13.5% experienced with the existing threat message. Instead of a survey design for phase 1, future research can implement an experimental design with random assignment to one of several different password threat messages in order to increase adoption rates beyond the paltry 13.5%. Future research can further investigate the perceived insufficient time and lack of immediacy issues by, possibly, demonstrating the quick installation and setup processes and/or manipulating installation time in a controlled experiment.

We believe that recent current events related to poor password management, such as the major password leaks at LinkedIn and resulting hack of FaceBook CEO Mark Zuckerberg's Twitter and Instagram accounts due to reuse of a weak password that was included in the LinkedIn data breach [32], will provide a more personal connection to home end-users and possibly reduce the effects of threat apathy on actual security behaviors. Password managers can help solve a real and important problem and it is important to theoretically and practically understand why home end-users are not adopting them. These types of systems may reduce information security breaches associated with poor password management practices.

7. References

[1] I. Ajzen, "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior", Journal of Applied Social Psychology, 32 (2002), pp. 665-683.

[2] C. L. Anderson and R. Agarwal, "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", MIS Quarterly, 34 (2010), pp. 613-643.

[3] C. J. Armitage and M. Conner, "Efficacy of the theory of planned behaviour: A meta-analytic review", British journal of social psychology, 40 (2001), pp. 471-499.

[4] S. Aurigemma, "A Composite Framework for Behavioral Compliance with Information Security Policies", Journal of Organizational and End User Computing, 25 (2013), pp. 32-51.

[5] A. Bandura, "Self-efficacy: toward a unifying theory of behavioral change", Psychological review, 84 (1977), pp. 191.

[6] T. Beardsley, R. Hodgman, J. Hart and H. Geiger, *The Attacker's Dictionary: Auditing Criminal Credential Attacks*, Rapid7, 2016, pp. 26.

[7] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", MIS Quarterly (May-2015 Forthcoming) (2015).

[8] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss, "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", European Journal of Information Systems, 18 (2009), pp. 151-164.

[9] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development*, Sage, 1998.

[10] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", MIS quarterly, 34 (2010).

[11] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", MIS quarterly, 34 (2010), pp. 523-548.

[12] Y. Chen, K. Ramamurthy and K.-W. Wen, "Impacts of Comprehensive Information Security Programs on Information Security Culture", Journal of Computer Information Systems, 55 (2015), pp. 11-19.

[13] Y.-Y. Choong and M. Theofanos, *What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter*, *Human Aspects of Information Security, Privacy, and Trust*, Springer, 2015, pp. 299-310.

[14] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin and R. Baskerville, "Future directions for behavioral information security research", Computers & Security, 32 (2013), pp. 90-101.

[15] R. E. Crossler, J. H. Long, T. M. Loraas and B. S. Trinkle, "Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap", Journal of Information Systems, 28 (2014), pp. 209-226.

[16] R. E. Crossler, J. H. Long, T. M. Loraas and B. S. Trinkle, "Understanding Compliance with BYOD (Bring Your Own Device) Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap", Journal of Information Systems (2014).

[17] CSID, *Consumer Survey: Password Habits - A study of password habits among American consumers*, 2012, pp. 10.
[18] J. D'Arcy, A. Hovav and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", Information Systems Research, 20 (2009), pp. 79-98.
[19] N. K. Denzin and Y. S. Lincoln, *The SAGE handbook of qualitative research*, Sage, 2011.
[20] J. Drennan, G. Sullivan and J. Previte, "Privacy, risk perception, and expert online behavior: An exploratory study of household end users", Journal of Organizational and End User Computing (JOEUC), 18 (2006), pp. 1-22.
[21] D. Florencio and C. Herley, *A large-scale study of web password habits*, *Proceedings of the 16th international conference on World Wide Web*, ACM, 2007, pp. 657-666.
[22] D. L. Floyd, S. Prentice-Dunn and R. W. Rogers, "A meta-analysis of research on protection motivation theory", Journal of applied social psychology, 30 (2000), pp. 407-429.
[23] R. Gross and A. Acquisti, *Information revelation and privacy in online social networks*, *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, ACM, 2005, pp. 71-80.
[24] D. Humphries, *Best Practices for Workplace Passwords*, in G. S. Advice, ed., 2015.
[25] A. Huth, M. Orlando and L. Pesante, *Password Security, Protection, and Management*, in U. S. C. E. R. T. (CERT), ed., 2013, pp. 5.
[26] I. Ion, R. Reeder and S. Consolvo, *"... no one can hack my mind": Comparing Expert and Non-Expert Security Practices*, *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 327-346.
[27] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study", MIS quarterly, 34 (2010).
[28] R. H. Kolbe and M. S. Burnett, "Content-analysis research: An examination of applications with directives for improving research reliability and objectivity", Journal of consumer research (1991), pp. 243-250.
[29] P. B. Lowry, C. Posey, R. B. J. Bennett and T. L. Roberts, "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust", Information Systems Journal, 25 (2015), pp. 193-273.
[30] Ofcom, *Adults' media use and attitudes (Report 2015)*, 2015, pp. 197.
[31] R. A. Peterson, "On the use of college students in social science research: Insights from a second-order meta-analysis", Journal of consumer research, 28 (2001), pp. 450-461.
[32] K. Rogers, *If Mark Zuckerberg Can Be Hacked on Twitter, So Can You*, *The New York Times*, The New York Times Company, www.nytimes.com, 2016, pp. 1.
[33] N. Rubenking, *Survey: Hardly Anybody Uses a Password Manager*, *SecurityWatch*, PC Magazine, 2015.
[34] R. A. C. Ruiter, L. T. E. Kessels, G.-J. Y. Peters and G. Kok, "Sixty years of fear appeal research: Current state of the evidence", International Journal of Psychology, 49 (2014), pp. 63-70.
[35] SANS, ed., *Password Construction Guidelines*, 2014.
[36] M. Siponen and A. Vance, "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations", European Journal of Information Systems, 23 (2014), pp. 289-305.
[37] T. F. Stafford and R. Poston, "Online security threats and computer user intentions", Computer (2010), pp. 58-64.
[38] E. Stobert and R. Biddle, *The password life cycle: user behaviour in managing passwords*, *Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 243-255.
[39] E. Vaast and E. Kaganer, "Social media affordances and governance in the workplace: An examination of organizational policies", Journal of Computer-Mediated Communication, 19 (2013), pp. 78-101.
[40] Verizon, *2016 Data Breach Investigations Report*, 2016.
[41] C. Vroom and R. Von Solms, "Towards information security behavioural compliance", Computers & Security, 23 (2004), pp. 191-198.
[42] R. Wash, E. Rader, R. Berman and Z. Wellmer, *Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites*, *Symposium on Usable Privacy and Security (SOUPS)*, 2016.
[43] K. Witte, G. Meyer and D. Martell, *Effective Health Risk Messages: A Step-By-Step Guide*, Sage Publications, 2001.
[44] M. Workman, W. H. Bommer and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test", Computers in Human Behavior, 24 (2008), pp. 2799-2816.
[45] L. Zeltser, *Password Managers*, *OUCH! The montly security awareness newsletter for computer users.*, SANS Institute, 2015.