American Psychological Association

Technology, Mind & Society
2021 Conference Proceedings

ISBN:

http://dx.doi.org/10.1037/xxxxxxx

Predicting the Adoption of Password Managers *

A Tale of Two Samples

Shelia M. Kennison[1] and D. Eric Chan-Tin[2]
[1]Oklahoma State University
[2]University of Loyola Chicago

Using weak passwords and re-using passwords can make one vulnerable to cybersecurity breaches. Cybersecurity experts recommend the adoption of password managers (PMs), as they generate and store strong passwords for all accounts. Prior research has shown that few people adopt PMs. Our research examined PM adoption in a sample of 221 undergraduates from psychology courses and a sample of 278 MTurk workers. We hypothesized that PM adoption could be predicted using a small set of user characteristics (i.e., gender, age, Big Five personality traits, number of devices used, frequency of using social media, and cybersecurity knowledge). The results showed that compared to students, MTurkers used more devices, used social media less often, had higher levels of cybersecurity knowledge, and were more likely to know what PMs are (93% vs. 33%). Of those who knew about PMs, only 40% of MTurkers and 47% of students reported using one. Those higher in cybersecurity knowledge were more likely to use PMs. Logistic multiple regression was used to predict which participants used PMs. The results showed that the results differed for MTurkers and students. For students, the model correctly classified 84.2% of participants; two predictors were significant. Those with higher levels of cybersecurity knowledge were more likely to use PMs, and those who used social media more often and were more likely to use PMs. For MTurkers, the model was not significant. The results may be useful to those who develop and implement campaigns to promote password managers and other recommended cybersecurity practices.

Keywords: technology adoption, cybersecurity, password managers, individual differences, cybersecurity knowledge

Cybersecurity breaches continue to threaten governments, corporations, and individuals. Breaches can occur when users re-use passwords (Stobert & Biddle, 2014) or use weak passwords that can be guessed or discovered using hacking software (Farcasin & Chan-Tin, 2015; Hitaj et al., 2019; Houshmand et al., 2015; Ji et al., 2015; Tatlı, 2015; Zhang et al., 2020). Among the recommended security practices is the use of Password Managers (PMs) (Security, 2021). PMs are used to store passwords used for all accounts and can be used to create new, strong passwords, reducing the risk of being hacked. The aim of the present study is to investigate whether PM adoption could be predicted using a relatively small set of personal characteristics (i.e., demographic variables, personality traits, number of devices used, and frequency of social media use).

Over the last decade, the number of PMs has increased. Many PMs are standalone applications that must be installed on devices. Others come pre-installed on devices. Despite the benefits of PMs and the availability of free and low cost PMs, there has not been widespread adoption of PMs (Alkadi et al., 2016; Aurigemma et al., 2017; Fagan et al., 2017; Pearman et al., 2019). Some of the most frequently given reasons for not adopting PMs include lack of awareness of PMs, their functions, and their benefits in protecting one from cybersecurity breacches (Aurigemma et al., 2017); lack of time and motivation (Alkadi et al., 2016; Fagan et al., 2017); and concerns about the security of PMs, specifically their vulnerability to being hacked (Pearman et al., 2019).

Relatively few studies have examined whether it is possible to predict use of PMs from personal characteristics. More studies have been conducted on predicting other cybersecurity behaviors

This article was published [to be completed by publisher].
(Shelia M.Kennison 0000-0001-9298-3152)
(D. Eric Chan-Tin 0000-0001-8367-5836)
This research was supported in part by [NSF DGE 1918591 & 1919004].
The authors have no conflicts of interest to disclose.

Correspondence concerning this article should be addressed to Shelia M. Kennison, Ph.D., Oklahoma State University, 116 Psychology Building, Department of Psychology, Stillwater, Oklahoma 74078, USA. Email: shelia.kennison@okstate.edu.

involving risk (e.g., using weak passwords, clicking links in emails, using unsecured WI-FI networks). For example, prior research supports the view that it may be possible to predict who will engage in risky cybersecurity behaviors. For example, research has suggested that older adults may engage in riskier cybersecurity behaviors than others (Whitty et al., 2015). Other research has observed that men report using risky cybersecurity behaviors more often than women (Anwar et al., 2017; c.f., Kennison & Chan-Tin, 2020). Studies have also shown that men report higher levels of cybersecurity knowledge than do women (Cain et al., 2018; Kennison & Chan-Tin, 2020). A growing number of studies support the assumption that those with higher levels of cybersecurity knowledge are less likely to engage in risky cybersecurity behaviors (Kennison & Chan-Tin, 2020; 2021; Whitty et al., 2015). However, earlier research showed that some users may engage in risky cybersecurity behaviors even when they know the behavior is risky (Notoatmodjo & Thomborson, 2009; Riley, 2006).

There has been interest in the relationship between cybersecurity behaviors and personality traits, such as Big Five personality traits (i.e., conscientiousness, emotional instability, agreeableness, extraversion, and openness). Several studies have found that those higher in conscientiousness reported engaging in risky cybersecurity behavior less often (Alohali et al. (2018; McCormac et al., 2017; Russell et al., 2015; Shappie et al., 2019). Others studies found that those higher in emotional instability engage in risky cybersecurity behaviors more often than others (Kennison & Chan-Tin, 2020; McCormac et al., 2017). A few studies have shown that those higher in agreeableness may be more aware of cybersecurity best practices (McCormac et al., 2017) and more likely to use them (Shappie et al., 2020). However, an intriguing study found that those higher in agreeableness were more likely to click on links in phishing attacks (Cho et al., 2016).

In the present study, we investigated whether we could predict the adoption of PMs using a small number of personal characteristics. These included cybersecurity knowledge, Big Five personality traits, number of devices used, frequency of social media use, gender and age. Because prior research has observed that personal characteristics (e.g., personality, gender, and age) can predict risky cybersecurity practices (Alohali et al., 2018; Anwar et al., 2017; Kennison & Chan-Tin, 2020; 2021; McCormac et al., 2017; Russell et al., 2015; Whitty et al., 2015), we reasoned that some of these personal characteristics may also predict adoption of PMs. We also reasoned that those with more devices may be more likely to adopt PMs, because having more devices requires the creation of more passwords. Lastly, we considered the possibility that frequency of social media use may be related to PM use. Those who use social media more frequently may more familiarity with cybersecurity generally and more knowledge about cybersecurity dangers.

In the reported study, we sampled two populations: a) undergraduates from psychology courses at a large public university and b) MTurk workers residing in the United States. For both samples, we tested five hypotheses: a) **t**hose with high levels of cybersecurity knowledge would be more likely to know about PMs and to adopt them; b) men would have higher levels of cybersecurity knowledge, be more likely to know about PMs, and more likely to adopt them; c) older adults would be less likely to know about PMs and would be less likely to use them; d) those with higher levels of conscientiousness would be more likely to know about PMs and to adopt them; e) those using more devices would be more likely to know about and to adopt PMs; and f) those using more social media platforms would be more likely to know about and to adopt them.

Method

Participants. 221 undergraduates from psychology courses participated in exchange for course credit. 278 MTurk workers participated for $2. After removing some participants as described later, there were 214 undergraduates and 275 MTurk workers. The mean age for the student sample was 18.8 years (SD = 1.25, Min = 18, Max = 25). The mean age for the MTurk sample was 38.6 years (SD = 11.94, Min = 20, Max = 73). Both samples were composed of a majority of White participants: MTurk sample -- 75% and SONA student sample -- 75%. The other ethnicities represented in the samples are as follows. MTurk sample -- 5% Latinx, 1% Native American, 6% African-American, 5% Asian/Asian-American, and 8% more than one category and SONA student sample -- 5% Latinx, 4% Native American, 4% African-American, 1% Asian/Asian-American, and 11% more than one category.

Procedure and Materials. We obtained IRB approval for the study prior to participant recruitment. In an online survey, implemented using a Professional license of Qualtrics, we assessed participants' knowledge of PMs, their use, their reasons for not using them, as well as their Big Five personality traits (using Saucier's 1994 mini-markers), cybersecurity knowledge, social media usage, age, and gender. Our student sample was recruited through a Department of Psychology SONA research pool, which included courses from psychology and speech communications. Many of these courses fulfilled general education requirements and included all majors on campus. Our MTurk workers were recruited through Amazon Mechanical Turk.

***PM Questions*.** Participants were asked if they knew what a PM was, if they use a PM, their reasons for not using a password manager, and the name of the PM they used (if they responded that they used one).

Social Media Questions. Participants were asked which social media platforms that they used. They also indicated their frequency of social media usage using a questions 6-point scale: *How often do you access your social media accounts: 1 = less than 30 minutes per day, 2 = between 30 minutes to 1 hour per day, 3 = between 1 hour and 2 hours per day, 4 = between 2 hours and 4 hours per day*, *5 = between 4 hours and 8 hours a day,* and *6= more than 8 hours per day*.

Cybersecurity Knowledge. We assessed cybersecurity knowledge using two measures from prior research. We used Parsons et al.'s (2017) 9-items related to password knowledge,

attitude, and behavior from the (HAIS-Q) (e.g., *It's acceptable to use my social media passwords on my work accounts* and *It's safe to have a work password with just letters*.), Participants rated their level of agreement of the statements on a 7-point scale (i.e., 1 = *Strongly Disagree*, 7 = *Strongly Agree*). The ordering of adjectives was randomized for each participant. Means were computed and some items were reverse scored. Larger means indicated higher levels of password knowledge, attitude, and behavior. Parsons et al.'s (2017) observed adequate internal consistency (i.e., Cronbach alphas over α = .70). As in Kennison and Chan-Tin, the internal consistency was adequate only when the 9 items were considered as a single factor (Cronbach alphas α = .71).

We also assessed cybersecurity knowledge using Kennison and Chan-Tin's (2020) 4-item measure. The questions were: a) *My knowledge of password security is high;* b) *Password security practices are not something that I have learned very much about* (reverse scored); c) *I know a lot about password security practices*; and d) *My level of knowledge about real world cases where sensitive data have been stolen by hackers is fairly high*. Participants rated their knowledge on a 7-point scale (1=*Strongly Disagree*, 7=*Strongly Agree*). The ordering of adjectives was randomized for each participant. Participants' responses were averaged with larger numbers reflecting higher levels of knowledge. Kennison and Chan-Tin (2020) observed good internal consistency (Cronbach α = .74) as we did in the present study (Cronbach α = .80).

Big Five Traits. We assessed personality using Saucier's (1994) 40-item mini-marker questionnaire, which is a popular measure of the Big Five personality traits (i.e., extraversion, conscientiousness, agreeableness, mood instability, and openness). Each of the five traits were assessed with eight adjectives, presented with a 9-point scale (*1=extremely inaccurate, 9=extremely accurate*). Participants were asked how well each adjective described them. The ordering of adjectives was randomized for each participant. After reverse scoring some items, we calculated the mean for each factor. Prior research has shown that the measure is associated with adequate internal consistency (Cronbach alphas between from 0.76 to 0.86, Mooradian & Nezlek, 1996). In the present research, we also observed adequate internal consistency (Cronbach alphas between α = .76 to α = .87).

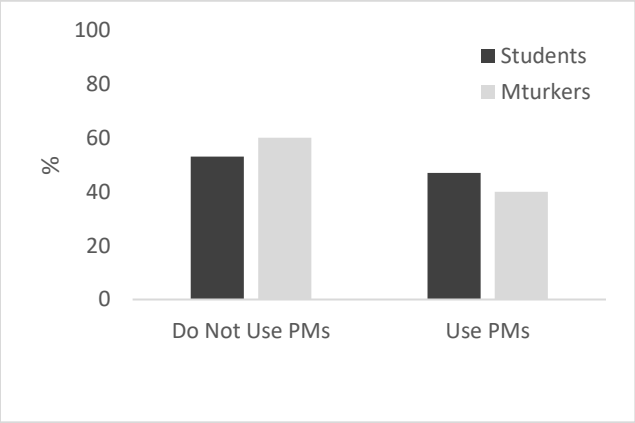
Demographic Questions. We asked participants to provide their age in years as two digits and their gender category (i.e., *man, woman, or a gender not listed*).

Attention Check Question. One question was used to catch inattentive responders: *Sometimes researchers include a question to determine if the participant is paying adequate attention while completing the survey. In order to show us that you are paying attention please select the fourth option as the response to this question*. The question was followed by a five possible responses: *1 = strongly disagree, 2 = slightly disagree, 3 = neither disagree nor agree, 4 = slightly agree*, and 5=*strongly agree*. The question appeared approximately in the mid-point of the survey and required a response.

Results

Participants who answered the attention check question incorrectly were excluded in the dataset (i.e., 7 undergraduates and 4 MTurk workers), which was then used to test the five hypotheses. Correlation results supported the hypothesis that cybersecurity knowledge would predict knowledge about PMs and adoption of PMs. Those with higher cybersecurity knowledge were more likely to know about PMs (Kennison & Chan-Tin questions: $r = .42$, $p < .001$ and HAIS-Q: $r = .31$, $p < .001$) and also more likely to use a PM (Kennison & Chan-Tin questions: $r = .19$, $p < .001$ and HAIS-Q: $r = .11$, $p = .013$). The results also indicated that MTurk workers had higher levels of cybersecurity knowledge than SONA students, as assessed by the two measures of knowledge were Parson et al.'s (2017) HAIS-Q ($t = 8.56$, $p < .001$, $\eta^2 = .13$) and Kennison and Chan-Tin's (2020) cybersecurity knowledge questions ($t = 12.96$, $p < .001$, $\eta^2 = .24$). MTurk workers were more likely to know about PMs than SONA students (93% vs. 33%), $t = 17.70$, $p < .001$, $\eta^2 = .41$. Of those who knew about PMs, PM adoption did not differ significantly for the two groups: MTurk workers: 40% vs. SONA students: 47%, $t = 1.47$, $p = .14$. Figure 1 displays use of PMs for the two groups. Table 1 displays the mostly frequently given reason.

Figure #. ***Password Manager Use by Type of Participant.***



Note. Figure displays percentages for those indicating that they knew about PMs. The differences between SONA students and MTurkers were comparable (i.e., not significant).

The results also confirmed the second hypothesis that men would report higher levels of cybersecurity knowledge than women: Kennison and Chan-Tin knowledge questions, $t = 7.91$, $p < .001$; knowledge of PMs ($t = -6.75$, $p < .001$, $\eta^2 = .09$), and be more likely to use of PMs than women were ($t = 1.97$, $p = .05$, $\eta^2 = .01$). Men also reported using more devices than women ($t = 2.20$, $p = .028$, $\eta^2 = .01$). However, women reported using social media more frequently than did men ($t = 2.35$, $p < .019$, $\eta^2 = .01$).

Table 1. ***Top Reasons for Not Using PMs***

Reasons for Not Using PMs
1. I don't know what a password manager is.
2. I don't want all my passwords in one place -- *What if the PM gets hacked?*
3. They cost too much.
4. I don't have time.
5. It's just another thing to have to keep up with.

Note. Order list the reason most frequently given to the least frequent.

The results disconfirmed the third hypothesis that knowledge of PMs and use of PMs would be lower for older participants. The results showed the opposite pattern. Age was positively correlated with knowledge of PMs ($r = .45$, $p < .001$) and use of PMs ($r = .18$, $p < .001$). It is worth noting that the MTurk sample had a much larger range of age than did the SONA student sample. There were relatively few participants older than 65 years in the MTurk sample and none in the SONA student sample

The results partially supported the fourth hypothesis that those higher in conscientiousness would be more likely to know about PMs and more likely to use them. Higher conscientiousness was related to knowledge about PMs, $r = .09$, $p = .038$, albeit weakly; however, there was no relationship between conscientiousness and use of PMs, $r = .02$, $p = .645$.

The results partially supported the hypothesis that those who using more devices would be more likely to know about PMs and to use them. Number of devices was weakly related to knowledge about PMs, $r = .11$, $p = .018$; however, there was no relationship between the number of devices used and use of PMs, $r = -.002$, $p = .959$. Overall, Mturkers used more devices than SONA students ($t = 2.25$, $p = .027$, $\eta^2 = .01$).

The results partially confirmed the fifth hypothesis that those who use social media more frequently would be more likely to know about PMs and to use them. SONA students who used social media more frequently were more likely to use PMs, $r = .15$, $p = .025$; however, there was no relationship between the frequency of using social media and knowledge of PMs, $r = .06$, $p = .38$. The relationships between social media use and knowledge about PMs and social media use and use of PMs were not significant for MTurkers. Overall, frequency of social media was not related to use of PMs, r = -.08, p = .08, but more frequent social media use was related to less knowledge about PMs, r = -.23, p < .001. The comparison of social media use for the two groups showed that Mturkers reported using social media less often than did SONA students ($t = -10.04$, $p < .001$, $\eta^2 = .17$).

Additional significant correlations were observed. Those higher in mood instability were less likely to know about PMs, $r = -.19$, $p < .001$ and less likely to use them, $r = -.10$, $p = .027$. Those higher in mood instability reported using social media more often, $r = .24$, $p < .001$. For MTurkers, those with lower levels of agreeableness were more likely to use PMs, $r = -.14$, $p = .024$.

Logistic multiple regression was used to predict which participants used PMs using type of participants, gender, age, number of devices, frequency of social media usage, Big Five personality traits, and cybersecurity knowledge as independent variables. PM use was coded as follows: 0 = does not use a PM, 1 = use a PM. Type of participant and gender were categorical predictor variables (type of participant: MTurkers = 0, SONA students = 1 and gender: 0=female, 1= male). The model was significant, $\chi2(11) = 35.80$ p < .001. The Nagelkerke estimated $R^2 = .11$. The model correctly classified 73.4% of participants. Type of participant ($B = .99$, $p < .001$) was significant. To explore the different patterns of results for the two groups of participants, we conducted separate logistic multiple regressions for the two groups. The model for MTurkers was not significant: MTurkers: $\chi2(11) = 11.10$, p = .435; however, the model for SONA students was significant: $\chi2(11) = 19.81$, p = .048. The Nagelkerke estimated $R^2 = .11$. The model correctly classified 84.2% of participants. There were two significant predictors: Cybersecurity knowledge ($B = .35$, $p = .028$) and frequency of social media use ($B = .54$, $p = .012$). Table 2 provides a summary of the logistic multiple regression analyses for the student and MTurk samples.

Table 2. ***Summaries of Logistic Multiple Regression Analyses for MTurk and Student Groups***

Student Sample	B	SE	Wald	Sig	Exp(B)	95% CI
HAIS-Q	.35	.51	.06	.81	1.13	.41-3.07
Cybersec Knowledge	**.35**	**.16**	**4.85**	**.028**	**1.41**	**1.04-1.92**
Agreeableness	.08	.19	.17	.68	1.08	.75-1.56
Extraversion	.16	.14	1.30	.26	1.17	.89-1.52
Conscientiousness	-.15	.22	.46	.50	.86	.56-1.33
Openness	.19	.29	.45	.50	1.21	.69-2.14
Mood Instability	-.32	.19	2.76	.097	.73	.50-1.6
Number of Devices	.09	.17	.24	.62	1.09	.78-1.53
Social Media Use	**.54**	**.21**	**6.24**	**.012**	**1.71**	**1.12-2.60**
Gender	1.23	.51	.06	.81	1.13	.42-3.07
Age	-.19	.19	.93	.33	.83	.56-1.22

MTurk Sample	B	SE	Wald	Sig	Exp(B)	95% CI
HAIS-Q	-.02	.17	.66	.42	1.29	.71-2.26
Cybersec Knowledge	.04	.13	.11	.74	1.04	.81-1.34
Agreeableness	-.25	.12	4.06	.04	.78	.62-.99
Extraversion	-.05	.08	.03	.85	.99	.84-1.16
Conscientiousness	-.05	.12	.16	.69	.95	.75-1.21
Openness	-.04	.11	.12	.73	.96	.78-1.19
Mood Instability	-.16	.10	2.33	.13	.86	.70-1.05
Number of Devices	-.19	.12	2.50	.11	.83	.66-1.21
Social Media Use	-.085	.14	.36	.55	.92	.70-1.21
Gender	.24	.29	.66	.42	1.27	.71-2.26
Age	.001	.01	.007	.93	1.00	.98-1.03

Note. Cybersec=Cybersecurity

Discussion

The study investigated whether a relatively small set of personal characteristics could predict who would know about PMs and use them. We tested five hypothesis. First, we expected those with high levels of cybersecurity knowledge would be more likely to know about PMs and to adopt PMs. Second, we expected that men would have higher levels of cybersecurity knowledge, be more likely to know about PMs, and more likely to use them. Third, we expected that those higher levels of conscientiousness would be more likely to know about PMs and to adopt PMs. Fourth, we expected that older participants would be less likely to know about PMs and to use them. Fifth, we expected those using more devices would be more likely to know about and to adopt PMs. Lastly, we expected those using more social media platforms would be more likely to know about and to adopt PMs. The results either confirmed or partially confirmed all but two of the hypotheses. Contrary to expectations, older participants were more likely to know about PMs and were also more likely to use them and more frequent use of social media predicted less knowledge about PMs. Among SONA students only, more frequent use of social media was related to use of PMs.

We found that those who reported higher levels of cybersecurity knowledge were more likely to know about PMs and also more likely to use them. Men reported higher levels of cybersecurity knowledge than women, were more likely to know about PMs and also more likely to use them. Those higher in conscientiousness were more likely to know about PMs, but not more likely to use them. Those who used more devices were more likely to know about PMs, but not more likely to use them. When multiple variables were considered together to predict use of PMs, different patterns were observed for MTurkers and SONA students. For SONA students, there were two significant predictors. Those with higher levels of cybersecurity knowledge were more likely than others to use a PM and those who use social media more frequently were less likely to use a PM. For MTurkers, the model was not significant. When considered with other variables, neither age nor gender was a significant predictor of PM adoption. Overall, MTurkers reported higher levels of cybersecurity knowledge and knowledge about PMs than SONA students, but the use of PMs did not differ significantly for MTurkers and SONA students.

Our results showing agreeableness was related to PM use among MTurkers who were found to have a relatively high level of cybersecurity knowledge are consistent with Cho et al.'s (2016) results showing that agreeableness related to falling for phishing attacks. Those lower in agreeableness with knowledge of cybersecurity issues may adopt a less cooperative interaction strategy online, viewing hacking as more common and being more cautious when interaction with unknown individuals. Or those higher in agreeableness may be more likely to adopt a cooperative interaction strategy online, viewing unknown others as unlikely to pose a cybersecurity threat.

The present results showing that PM use is predicted by a few personality variables (i.e., only agreeableness) contrast with prior research showing more robust personality effects in predicting other cybersecurity behaviors (e.g., using strong passwords and clicking on phishing links). We suggest that it may be the case that personality traits are less likely to predict behaviors, which require more decision-making time and effort and involve consideration of many factors, including financial cost. When deciding to use a PM, one must identify one to use, download/install it, and input all of one's current passwords into it. Committing to use a PM requires a significant time commitment initially. In addition, there is sometimes a financial cost to adopting a PM. In terms of both time and money, those who end up adopting a PM may do so after a considerable about of contemplation. Other cybersecurity behaviors (e.g., using strong passwords or not clicking on phishing links), can be done relatively quickly, involving minimal cognitive effort, and involving the consideration of fewer relevant factors.

These results are important because no known prior study has shown that knowledge or use of PMs could be predicted by personal characteristics. The results have important implications for cybersecurity training efforts as well as messaging that might encourage and/or incentivize people to start using PMs. The strong relationship between cybersecurity knowledge and PM use suggests that providing more people with routine and/or enhanced cybersecurity education could lead to more PM use. When approaching individuals with a relatively low level of cybersecurity knowledge, such as our sample of undergraduates from psychology courses, one may find it possible to increase adoption of PMs by providing foundational cybersecurity knowledge. It may also be beneficial to tie in discussions of PMs with the topic of social media use and the possibility of using additional devices in the future. Student may begin to think about their future needs for numerous passwords and possible strategies for protecting themselves from cybersecurity breaches not only in the present time but also in the future. Most individuals using just one or two devices and/or social media platforms now may be easily persuaded that in future months or years, they will likely be using more devices and/or more social media platforms. Adopting a PM now can help protect them both now and in the future, when they will likely have an even greater number of passwords. For individuals identified as having a medium to high level of cybersecurity knowledge about PMs, such as our sample of MTurk workers, a useful strategy might involve targeting individuals higher in agreeableness with messaging that highlights reasons that it is good to be less cooperative with others online, because some individuals may have nefarious motives, such as hacking.

The strategy of using a relatively small set of personal characteristics to select individuals for enhanced cybersecurity training could be automated, saving organizations tame and money. The enhanced cybersecurity training may describe the value of PMs generally, but also recommend specific PMs, which are most likely to be compatible with the technology systems used in the organization. Individuals who are targeted for supplemental

cybersecurity training may not even become aware that they have been targeted; rather, they are likely to view such training as required by all members of the organization.

There were limitations of the present study. A major limitation relates to the fact that we relied on self-report measures. Some participants may not provide accurate responses. Sometimes responses may be influenced by social desirability bias, as respondents may report traits and behaviors that they perceive to be more acceptable to others, particularly the researchers. Using a PM and reporting higher levels of cybersecurity knowledge might have been perceived as socially desirable. Future studies may include one or more measures to assess social desirability bias generally. Such measures enable researchers to exclude participants demonstrating high levels of social desirability bias. A second concern with self-report measures is that it is also possible that responses can be inaccurate due to memory errors. Some respondents may have reported using PMs when they had not. They may also have made inaccurate estimations for other variables (e.g., frequency of social media use) due to poor remembering. Future research in the field in which participants' use/non-use of PM can be objectively confirmed may be useful. Such research may find that daily reliance on PMs is actually lower than the present study suggests. Moreover, it is important to know how much participants are using PMs (for every password, only for the important account, or occasionally) and also whether they allow the PMs.

References

Alkaldi, N., & Renaud, K. (2016). Why do people adopt, or reject, smartphone password managers? In Proceedings of the 1st European Workshop on Usable Security (EuroUSEC '16).

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security, 26*(3), 306-326. https://doi.org/10.1108/ICS-03-2018-0037

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 6*9, 437-443.

Aurigemma, S., Mattson, T., & Leonard, L. (2017). So much promise, so little use: What is stopping home end-users from using password manager applications? Proceedings of the 50th Hawaii International Conference on System Sciences.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications, 42*, 36-45.

Cho, J. H., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. March2016 IEEE International multi-disciplinary conference on cognitive methods in situation awareness and decision support (CogSIMA)(pp. 7–13). IEEE.http://dx.doi.org/10.1109/COGSIMA.2016.7497779.

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. Human-centric *Computing and Information Sciences, 7*(1), 1-20. https://doi.org/10.1186/s13673-017-0093-6

Farcasin, M., & Chan-Tin, E. (2015). Why we hate IT: Two surveys on pre-generated and expiring passwords in an academic setting, Wiley Security and Communication Networks, n/a, 10.1002/sec.1184.

Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019). Passgan: A deep learning approach for password guessing. In International Conference on Applied Cryptography and Network Security (pp. 217-237). Springer.

Houshmand, S., Aggarwal, S., & Flood, R. (2015). Next gen PCFG password cracking. *IEEE Transactions on Information Forensics and Security, 10*(8), 1776-1791. https://doi.org/10.1109/TIFS.2015.2428671

Ji, S., Yang, S., Hu, X., Han, W., Li, Z., & Beyah, R. (2015). Zero-sum password cracking game: A large-scale empirical study on the crackability, correlation, and security of passwords. *IEEE Transactions on Dependable and Secure Computing, 14*(5), 550-564. https://doi.org/ 10.1109/TDSC.2015.2481884

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using personal characteristics and knowledge to predict cybersecurity behaviors. *Frontiers in Psychology, 11*:546546. https://doi.org/10.3389/fpsyg.2020.546546

Kennison, S. M., & Chan-Tin, E. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports, 4*: 100132. https://doi.org/10.1016/j.chbr.2021.100132

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. In Proceedings of the Seventh Australasian Conference on Information Security-Volume 98 (pp. 71-78). Australian Computer Society, Inc.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019, August). Why people (don't) use password managers effectively. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA (pp. 319-338).

Pew Research Center. (2017). Americans and cybersecurity. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Riley, S. (2006). Password security: What users know and what they actually do. *Usability News, 8*(1), 2833-2836

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology, 1*(3-4), 163-174. https://doi.org/10.1080/23742917.2017.1345271

Saucier, G. (1994). Mini-Markers: A brief version of Goldberg's unipolar big-five markers. *Journal of Personality Assessment, 63*(3), 506-516. https://doi.org/10.1207/s15327752jpa6303_8

Security. (2021, May 6). Best practices during World Password Day. *Security.* https://www.securitymagazine.com/articles/95118-best-practices-during-world-password-day

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture*, 9(4), 475–480. https://doi.org/10.1037/ppm0000247

Stobert, E., & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In 10th Symposium on Usable Privacy and Security (SOUPS 2014) (pp. 243-255).

Tatlı, E. I. (2015). Cracking more password hashes with patterns. *IEEE Transactions on Information Forensics and Security, 10*(8), 1656-1665. https://doi.org/10.1109/TIFS.2015.2422259

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 3-7. https://doi.org/10.1089/cyber.2014.0179

Zhang, J., Yang, C., Zheng, Y., You, W., Su, R., & Ma, J. (2020). A Preliminary Analysis of Password Guessing Algorithm. In 2020 *29th International Conference on Computer Communications and Networks* (ICCCN) (pp. 1-9). IEEE. https://doi.org/10.1109/ICCCN49398.2020.9209690

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., & Schaub, F. (2020, April). Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-15).