Personality and Cognitive Factors in Password Security Behaviors

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

Prior research has suggested that cognitive factors, such as memory ability, would be related to how people make passwords; however, few studies have assessed cognitive factors in a study in which participants created passwords. In an online study, we asked participants to create three new passwords and to rate the likelihood that they would re-use a password in the future and share passwords with others in the future. We also assessed participants' self-reported everyday memory failures, their motivation to engage in cognitive processing (also called need for cognition), their general risk-taking in daily life, and their password security knowledge. We found that participants created stronger passwords for the banking and email apps than for the social media app. Further, those reporting more frequent memory failures in daily life created the weakest passwords, and those who were highest in need for cognition created stronger passwords than others. The results highlight the need to educate users about how they make themselves vulnerable to cyber security breaches on multiple accounts when any one account of theirs is breached (i.e., credential stuffing). Institutions may be able to use incorporating information about the everyday memory failures and need for cognition in their cybersecurity educational programs.

Keywords: Cybersecurity; Passwords; Memory Problems; Need for Cognition; College Students

Cybersecurity breaches remain a threat to individuals as well as institutions. The cost of breaches continues to rise annually (Ponemon Institute, 2019; 2021). The cost of cybersecurity breaches occurring since the beginning of the COVID-19 pandemic increased more for institutions with a greater percentage of their members working remotely (Ponemon Institute, 2021). Across institutions, the most frequent type of initial attack was the use of compromised credentials (e.g., passwords). Among the most frequent targets of attacks were educational institutions, including colleges and universities. There is a growing body of research on the cybersecurity behaviors of students and institutional strategies for

Author info: Correspondence should be sent to: Shelia Kennison, 116 Psychology Building, Oklahoma State University, Stillwater, Oklahoma 74078
Shelia.kennison@okstate.edu
North American Journal of Psychology, 2023, Vol. 25, No. 3, 599-618.
© NAJP

strengthening students' cybersecurity knowledge and behavior (Aljohni, et al., 2021; Alqahtani, 2022; Al-Zahrani, 2015; Cordova et al., 2017; Dunaway & Macharia, 2021; Kennison & Chan-Tin, 2020; Kennison et al., 2021; Pawlowski & Jung, 2015; Peker et al., 2016; Tick et al., 2021; Xu et al., 2019; Yan et al., 2021; Zwilling et al., 2022). The aim of the present research was to examine the factors related to college students' cybersecurity behavior, specifically knowledge about and creation of new passwords.

Prior examinations of breaches affecting major corporations have found that some occurred due to hackers exploiting weak passwords (e.g., Solarwinds: Afifi-Sabet, 2021; Godaddy: Cluley, 2021; Equifax: O'Flaherty, 2019; Target: Plachkinova & Maurer, 2019). Recent analyses of the most frequently used passwords demonstrate that many people still use easily guessed weak passwords (Meyer, 2022; Veroni et al., 2022). When weak passwords are used, they can be guessed or cracked (also called credential cracking, Ba et al., 2021) by cyber criminals who often rely on algorithms (Farcasin & Chan-Tin, 2015; Hitaj et al., 2019; Zhang et al., 2020). Cyber criminals are also known to use individuals' previous passwords, which have been revealed publicly in hacks, to guess passwords for specific users' other accounts (also called credential stuffing, Ba et al., 2021; See also Haque et al., 2013). In an analysis of the credentials leaked online from major breaches, Meyer (2020) reported the top ten most commonly used passwords from publicly available breaches to be as follows: *123456*, *123456789*, *qwerty*, *password*, *12345*, *qwerty123*, *1q2w3e*, *12345678*, *111111*, and *1234567890.* Security experts recommend using a different strong password for each account (Grassi, 2020). A strong password would be one with a mixture of numbers, lowercase letters, uppercase letters, and symbols that does not contain common words or names. Longer passwords are generally stronger than very short passwords (Wheeler, 2016).

Institutions routinely rely on training to raise awareness about cybersecurity and to reduce how often members of their organizations engage in risky cybersecurity behaviors; however, some studies suggest that training may not always be effective as users engage in risky cyber behavior even after training (Bada et al., 2015; Cain et al., 2018; Lorenz et al., 2013; Riley, 2006). Some researchers have pointed out that institutions may not be doing enough to provide their members with adequate communications about cyber security (Adams & Sasse, 1999). Studies have observed that those with more knowledge about cyber security are less likely to engage in risky cyber security behavior (Kennison & Chan-Tin, 2020; McCrohan et al., 2010; Peker et al., 2016). Prior research has suggested that men tend to have more knowledge than

women (Cain et al., 2018; Kennison & Chan-Tin, 2020), but may be more likely thaan women to engage in risky cybersecurity behavior (Anwar et al., 2017; Gratian et al., 2018).

Researchers have explored the relationship between personal characteristics, such as personality traits, and cybersecurity behavior with the rationale that enhanced cybersecurity training could be directed to individuals' most likely in need of it (Alohali et al., 2018; Kennison & Chan-Tin, 2020; Kennison et al., 2021; Russell et al., 2017; Shappie et al., 2019). Studies have found that those who are higher in conscientiousness are less likely engage in risky cyber security behavior (Alohali et al., 2018; Kennison & Chan-Tin, 2020; Kennison et al., 2021; Russell et al., 2017; Shappie et al., 2019) and those with higher levels of emotional instability (also called neuroticism) are more likely to engage in risky cybersecurity behavior (Kennison & Chan-Tin, 2020; Kennison et al., 2021; Shappie et al., 2019). Kennison and Chan-Tin (2020) found that those higher in sensation-seeking personality traits, which have been linked to more frequent risk-taking, took more cyber security risks than others. In the same study, those who reported engaging in more general risk-taking in daily life also reported being more likely to take more cyber security risks, a finding also observed by Kennison et al. (2021).

The purpose of the present research is to examine a neglected area in applied cognitive psychology. Of interest was how individual differences in personality and cognitive factors relate to behaviors involved in cybersecurity behaviors, specifically the creation of passwords. The creation of a password can be as complex as involving at least three steps (e.g., Camp et al., 2016): a) thinking up a password; b); remembering the password and c) associating the password in memory with the particular context (i.e., which account it can access). Most prior research on how people create passwords has been carried out by researchers from computer science and has not prioritized developing process models to describe different stages involved in password creation and how individual difference variables might be involved in these stages.

We reasoned that individuals are likely to use different passwords strategies for different types of accounts, using stronger passwords for apps linked to financial information (e.g., credit card or banking information) than for other types of apps. Few studies have examined the possibility that people tend to use different levels of password security for different types of accounts. In one prior study in which researchers examined password behavior of clients after they installed a new Microsoft-related application, Florencio and Herley (2007) found that participants tended to create weaker passwords for a New York Times subscription as compared with the overall average password strength for other types of apps, which included Outlook work email, Paypal, and

Fidelity. The passwords for Paypal and Fidelity, both of which are financial apps, were stronger as compared with the overall average password strength for other apps. Clients used the strongest passwords for their Outlook work email, which had password requirements (i.e., uppercase letters, lowercase letters, and special characters). Our reasoning that users create stronger passwords for some accounts and create weaker passwords for others is compatible with the protection motivation theory (Rogers, 1975) as applied to how users decide whether to engage in cybersecurity-related behaviors (Debb & McClellan, 2021). Specifically, users evaluate their vulnerability (i.e., threat appraisal) and determine if/how to act in the context. We reason that an important aspect of the threat appraisal in creating new passwords is the type of account for which one is creating a new password. Users may view their vulnerability to adverse consequences from hacking to be higher for some accounts (e.g., banking app) than for others (e.g., social media app or email app).

In the present study, we examined the roles of personality and cognitive factors in password security behaviors. We considered the strong possibility that individuals who experience problems with remembering in daily life, may differ from others when creating new passwords. For example, they may create passwords that are easier to remember, which may end up being weak passwords. They may also be more likely to reuse previously used passwords. Memory research supports the view that long-term memories, which can be retained permanently, are first processed in working memory, which is limited in capacity and available for only a brief time (Cotton & Ricker, 2022; Forsberg et al., 2021). Some information processed in working memory will not be transferred to long-term memory (i.e., will be forgotten). Those with smaller working memory capacities may have to put in more effort to transfer the information to long-term memory. On the other hand, it is also plausible that individuals with memory problems may take more steps to create especially strong passwords because they have developed strategies in daily life for compensating for their memory weaknesses. Prior research has discussed how memory ability might influence cyber security behavior (Camp et al., 2016; Gao et al., 2018; Pilar et al., 2012; Vu et al., 2007; Woods & Siponen, 2018). In a study of adults varying in age from 18 to 93 years, Pilar et al. (2012) found that those with more accounts reported having more memory problems with their passwords specifically (i.e., not about their general memory problems in daily life) and were more likely to keep a written record of their passwords. We are aware of no prior study that has shown that general memory problems in daily life relate to individuals' password security behaviors.

The present study also examined how individuals differing in how much they enjoy thinking (also called need for cognition, Cacioppo & Petty, 1982) might differ in their password creation. A contemporary view of need for cognition is that it is a personality trait related to how motivated individuals are to engage in mental effort (Cacioppo & Petty, 1982; Gärtner et al., 2021). Other research has shown individual differences in the need for cognition to be positively somewhat related to fluid intelligence, but unrelated to working memory capacity (Fleischhauer et al., 2009; Gärtner et al., 2021). Recent research by Kennison et al. (2021) found that those reporting higher levels for need for cognition created stronger passwords. Following these results, we reasoned that individuals who are higher in need for cognition may be more motivated to think about cybersecurity, generally, and also be more motivated to think about how best to make a new password for different types of apps, specifically.

In the reported study, we examined personality and cognitive factors in password security behavior. We tested four sets of hypotheses. We hypothesized that participants would create stronger new passwords for a new banking app or a new email app than a new social media app. In addition, we hypothesized that those reporting more frequent memory problems would create weaker passwords, as such passwords may be easier to remember. Those reporting more frequent memory problems may also be more likely to use the same passwords for the three new apps and report greater likelihood to reuse passwords. We also hypothesized that those higher in need for cognition would be more likely to create stronger passwords (Kennison et al., 2021), as they may engage in more thinking during the password creation process and cybersecurity generally. We also hypothesized that those higher in need for cognition would be less likely to use the same password for the three new apps, report lower likelihood of reusing passwords and sharing passwords in the future. We also hypothesized that those reporting higher levels of general risk-taking would create weaker passwords (c.f., Kennison & Chan-Tin, 2020; Kennison et al., 2021), be more likely to use the same passwords for the three new apps, and report greater likelihood to share and reuse passwords. Lastly, we hypothesized that men would report higher levels of cybersecurity knowledge than women and be more likely to engage in risky cybersecurity behaviors (c.f., Kennison & Chan-Tin, 2020), such as creating weak passwords, being more likely to share and reuse passwords in the future.

METHOD

Participants

Four hundred forty four (114 men, 327 women, and 3 other) undergraduates participated in exchange for course credit. The mean age was 20.27 years (*SD* = 4.48). The sample was majority White (73%). Other groups in the sample included Hispanic (6%), Black (4.2%), Native American (5.2%), Asian/Asian-American (2%), Pacific Islander/Native Hawaiian (1%), and more than one category (8.6%).

Materials

We asked participants to create three new passwords, which they entered in to three text boxes. The instructions were as follows:

> Take a moment and imagine that you have downloaded three new applications. You are asked to create passwords for these applications so that you can access them in the future. Please enter three passwords below that are typical of the passwords that you use in your daily life. One is for a new banking app, one for new social media platform, and one for a new email account.

We used measures from prior research to assess everyday memory failures, need for cognition, and password security knowledge. We used the 28-items of the M*emory Failures of Everyday* (MFE) from Montejo Carrasco et al. (2012), which were derived from previous work beginning with Sunderland et al. (1983). Each of the 28 items described an example of everyday memory failure (e.g., *Forgetting where you have put something* and *Finding that a word is "on the tip of your tongue")* was presented with a 3-point rating scale: 1) never, 2) sometimes, not often and 3) frequently, often. Participants were instructed to rate how frequently they experienced each of the examples of memory failure. Ratings were averaged for each participant with higher numbers reflecting more frequent memory failure. The measure has demonstrated high internal consistency in prior research (Cronbach alpha $\alpha = .90$, Montejo Carrasco et al., 2012). We found that the measure demonstrated high internal consistency (Cronbach $\alpha = .91$).

We used Cacioppo and Petty's (1982) 18-item *Need for Cognition* questionnaire to assess individual differences in cognition. Each statement was rated on a 5-point scale (i.e., *1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree Nor Disagree, 4 = Disagree, 5 = Strongly Agree*). Example statements include *I would prefer complex to simple problems* and *I really enjoy a task that involves coming up with new solutions to problems*. For each participant, the average rating was computed after reverse scoring some items. Higher averages indicated more need for cognition. The measure has demonstrated high internal

consistency in prior research (Cronbach alpha α = .90, Cacioppo et al., 1982; 1984). We found that the measure demonstrated high internal consistency (Cronbach α = .85).

We assessed cybersecurity knowledge using four questions previously used by Kennison and Chan-Tin (2020): a) *My knowledge of password security is high*; b) *Password security practices are not something that I have learned very much about*; 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 indicated their level of agreement using a 7-point scale (*1=Strongly Disagree, 2 = Disagree, 3 = Slightly Disagree, 4 = Neither Disagree Nor Agree, 5 = Slightly Agree, 6 = Agree, 7=Strongly Agree*). We calculated the average rating, after reverse scoring one item. Prior research observed adequate internal consistency for the items (Cronbach α = .74, Kennison & Chan-Tin, 2020). In the present study, we also observed good internal consistency (Cronbach α = .82).

We constructed a question to assess participants' likelihood of using the same password on multiple apps in the future. The instructions were as follows: *Please take a few minutes to consider how likely you are to re-use an old password for each of the following "new" situations.* Participants rate the likelihood on a 5-point scale (i.e*., 1 = not at all likely, 2 = somewhat unlikely, 3 = neither likely nor unlikely, 4 = somewhat likely, 5 = very likely*). Participants rated six new situations: a new phone, a new tablet, a new banking app/website, new email account, and new gaming app/website. Average likelihood was computed for each participant with higher averages reflecting greater likelihood to share re-use passwords. We found that the question demonstrated adequate internal consistency. The Cronbach alpha was .92.

We constructed a question to assess participants' likelihood of sharing passwords with others in the future. The instructions were as follows: *Please take a few minutes to consider how likely you are to share one or more of your passwords with the person listed below*. Participants rate the likelihood on a 5-point scale (i.e*., 1 = not at all likely, 2 = somewhat unlikely, 3 = neither likely nor unlikely, 4 = somewhat likely, 5 = very likely*). Participants rated ten types of others: *mother or father, sibling, roommate/housemate, work colleague who is interacted with regularly, work colleague interacted with rarely, boss, best friend, stranger who requests it on a phone call, a stranger who identifies themselves as an IT employee hired by your company, and any other family member (e.g., aunt, uncle, cousin, grandparents*). Average likelihood was computed for each participant with higher averages reflecting greater likelihood to share passwords. We found that the

question demonstrated adequate internal consistency. The Cronbach alpha was .813.

We used an attention check question in order to identify inattentive responders. The instructions were as follows: *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.* These instructions were followed by a 5-point scale (i.e., *1 = strongly agree, 2= slightly agree, 3 = neither agree nor disagree, 4 = slightly disagree, 5 = strongly disagree*). We also asked participants to indicate their gender (i.e., male, female, or other), their age in years, and their ethnicity.

Procedure

After we obtained IRB approval for the study, we recruited participants from a research participant pool (i.e., SONA system) housed in a department of psychology. The majority of participating courses were general education courses, attracting all majors on campus. Participants completed our online survey, which was implemented with a professional license of Qualtrics. Participants received the questions in the same order (i.e., personality, need for cognition, new password creation, memory problems, future password sharing, future password reuse, and demographics).

We assessed password strength using Wheeler's (2016) zxcvbn algorithm, which scores password strength using integers ranging from 0 (weakest) to 4 (strongest) and provides information about the average number of guesses and approximate amount of time that it would take to guess the password. We carried out statistical analyses using IBM's SPSS Statistics software version 26. We analyzed descriptive statistics for the data, including means, standard deviations, and correlation. We also carried out multiple regressions. The data, methods, and materials from this study are available from the corresponding author upon request.

RESULTS

Responses of participants who failed to answer the attention check question correctly (i.e., 7 men and 18 women) were eliminated from the dataset. The remaining data were used to calculate means, standard deviations, and Pearson's r values. To test the hypothesis that participants would create stronger passwords for a new banking app or a new email app than for a new social media app, we carried out a one-way Analysis of variance (ANOVA). The results showed that passwords created for a new banking app were stronger than those created for a new social media app (banking app: 3.35 vs. social media app: 3.19), F (1,

373) = 10.66, $p < .001$, but were not stronger than those created for a new email app (banking app: 3.35 vs. email app: 3.41), F (1, 373) = 1.22, p = .268. The passwords created for a new email app were stronger than those created for the new social media app (social media app: 3.19 vs email app: 3.41), F (1.373) = 21.64, $p < .001$.

Memory Failures and Password Strength

To test the hypothesis that those reporting having memory failures more often would create weaker passwords, we examined the correlations. Table 1 displays the results of correlations between need for

Table 1. Summary of Correlational Results for Women (Men)

Variables	Need for Cognition	Memory Failures	General Risk-Taking
PW Strength Banking	.20** (.25*)	-.15** (-.18**)	.05 (-.22*)
PW Strength Email	.19** (.25*)	-.17** (-.16*)	.07 (.04)
PW Strength Social	.16** (.27*)	-.08 (.006)	.06 (-.003)
Made Different PWs	.07 (.003)	-.09 (.03)	-.15* (-.003)
Future PW Sharing	.02 (.14)	.008 (.21*)	.06 (.28**)
Future PW Re-Use	-.03 (-.06)	.04 (-.05)	.01 (-.03)
Cyber Knowledge	.04 (.26**)	-.06 (.12)	-.03 (-.13)

Note: PW = password *$p < .05$, **$p < .01$, ***$p < .001$

cognition and everyday memory failures for women and men. The results supported the hypothesis, showing that those with more memory failures created weaker passwords for the banking app, r = -.17, p = .001 and the social media app, r = -.175, p = .001. When men's and women's passwords were considered separately, the relationships were observed for women only: banking app, r = -.15, p = .01 and the social media app: r = -.17, p = .005. Correlational results provided no support for the hypothesis that those reporting more frequent memory failures would also report being more likely to reuse passwords in the future. We also found that those reporting more frequent memory failures would also report being more likely to share passwords in the future. The relationship was observed for men only (r = .21, p = .03).

Need for Cognition and Password Strength

Correlational results also provided support for the hypothesis that those higher in need for cognition would create stronger passwords. The relationships were observed for each of the three apps (banking app: r = .22, $p < .001$, social media app: r = .21, $p < .001$, email app: r = .20, $p <$ .001). When men's and women's passwords were considered separately,

the relationships were observed for men (banking app: r = .25, p = .017, social media app: r = .25, p = .018, email app: r = .27, p = .011) and for women (banking app: r = .20, p = .001, social media app: r = .19, p = .002, email app: r = .16, p = .007). The results did not support the hypothesis that those higher in need for cognition would be less likely to repeat a password when they created new passwords for the banking, social media, and email app, would be less likely to share passwords in the future, or would be less likely to re-use passwords in the future.

Risk-Taking and Password Strength

The correlational results also provided partial support for the hypothesis that those reporting higher levels of general risk-taking would create weaker new passwords. The relationship was observed only for men for the banking app only (r = -.22, p = .034). There was partial support for the hypothesis that those reporting higher levels of general risk-taking would be less likely to create different passwords for the three new apps. The relationship was observed only for women (r = -.15, p = .014). There was support for the hypothesis that those reporting higher levels of general risk-taking would be more likely to share passwords in the future, r = -.13, p = .01. When men's and women's passwords were considered separately, the relationship was observed only for men (r = .28, p = .005). There was no support for the hypothesis that those reporting higher levels of general risk-taking would be more likely to reuse passwords in the future.

Gender and Password Strength

To test the hypothesis that men would create stronger passwords than women, we compared means using *t*-tests. The results partially supported the hypothesis. Men created stronger passwords for a new email app than did women (men: 3.67 vs. women: 3.31, t = 2.91, p = .004. The passwords for the other two apps showed similar trends, but the differences were not significant: banking app (men: 3.51 vs women: 3.28, t = 1.85, p =.066) and social media app (men: 3.35 vs women: 3.13, t = 1.76, p = .079). The results also supported the hypothesis that men would report higher levels of cybersecurity knowledge than women (men: 4.01 vs women: 3.24, t = 5.08, p < .001). The results supported the hypothesis that women would report being more likely to re-use passwords in the future (women: 4.14 vs men: 3.91, t = 2.01, p = .046). The results failed to support the hypothesis that women would report being more likely to share passwords in the future (women: 2.01 vs men: 1.99, t = .23, p = .83).

Multiple Regression Analyses

To explore further how cybersecurity knowledge, need for cognition, and everyday memory failures relate to password strength and likelihood to share and reuse passwords in the future, we carried out multiple regression analyses. First, we used the average password strength for the three new apps as the dependent variable and gender, cybersecurity knowledge, everyday memory failures, and general risk-taking as the

Table 2. Summary of Multiple Regression Results for Variables Predicting Average Password Strength and Likelihood of Future Reuse of Passwords

Predicting Average Password Strength

	β	t	sr^2	R	R^2	ΔR^2
Variables				.31	.08	.10***
Gender	.06	1.17	.003			
Cyber Knowledge	.10	1.92	.009			
Need for Cog	.21	4.16*	.043			
Memory Failures	-.13	-2.45*	.014			
Risk-taking	.06	1.12	.003			

Predicting Likelihood of Future Reuse of Passwords

	β	t	sr^2	R	R^2	ΔR^2
Variables				.26	.06	.07***
Gender	-.04	-.74	.001			
Cyber Knowledge	-.25	-4.98***	.057			
Need for Cog	-.02	-.31	.000			
Memory Failures	.002	.34	.000			
Risk-taking	-.023	-.47	.000			

Note: Cyber = Cybersecurity, Cog = Cognitive, *p < .05, **p < .01,***p < .001

independent variables entered simultaneously. The model was significant, $F(5, 369) = 21.53$, $p < .001$, accounting for 10% of the variance in average password strength. There were two significant predictors: need for cognition ($\beta = .21$, $p < .001$) and everyday memory failures ($\beta = -.125$, $p = .015$). Secondly, we used likelihood to re-use passwords in the future as the dependent variable and gender, cybersecurity knowledge, everyday memory failures, and general risk-taking as the independent variables entered simultaneously. $F(5, 407) = 5.90$, $p < .001$ accounting for 7% of the variance in average password strength. The only significant predictor was cybersecurity knowledge (β

= -.25, $p < .001$). Lastly, we used likelihood to share passwords in the future as the dependent variable and gender, cybersecurity knowledge, everyday memory failures, and general risk-taking as the independent variables entered simultaneously. The model was not significant, $F(5, 409) = 1.99$, $p = .079$. Table 2 displays the results for the analyses predicting average password strength and likelihood to reuse passwords in the future.

GENERAL DISCUSSION

The study investigated how personality and cognitive factors are related to individuals' cybersecurity behaviors. We assessed whether the passwords that participants created for new apps would vary depending on the type of app and whether password strength would be related to individual differences in need for cognition, everyday memory failures, and in password security knowledge. The results confirmed that participants created the weakest passwords for a new social media app and stronger passwords for a new banking app and a new email app. These results are consistent with Florencio and Henley's (2007) findings showing that passwords created for Outlook work email and for Paypal and Fidelity accounts were stronger than for a New York Times subscription. We suggest that the results are compatible for protection motivation theory as applied to cybersecurity decisions (Debb & McClellan, 2021). Users' view of their vulnerability to hacking may vary across different types of apps. Apps that are linked with financial information may be viewed as a high priority for cybersecurity measures, while other apps may be viewed as a low priority. Nevertheless, when they use weak passwords for some apps and strong passwords for other apps, users can fall victim to credential stuffing (Ba et al., 2021), which could result in a password obtained from an app perceived as a low priority for cybersecurity to be used to guess passwords for apps that are perceived as a high priority for cybersecurity (e.g., banking app).

The results showed that those who reported experiencing more everyday memory failures in daily life created weaker passwords overall. Our results further showed that individuals reporting more daily memory failures created weaker passwords than others. Correlational results showed that women reporting more everyday memory failures created weaker passwords for a new banking app and new social media app, and men who reported more everyday memory failures also reported being more likely to share passwords with others in the future. Those experiencing memory problems may engage in risky cybersecurity strategies with regard to passwords (i.e., using passwords that are easier to remember, which may be weaker, and/or re-using passwords).

Our results also showed that individual differences in propensity to engage in thinking are related to password strength. We found that those

reporting higher levels of need for cognition, the personality trait reflecting individual differences in motivation to engage in thinking, created stronger passwords for each of the three new apps. Cyber security education programs or trainings may be able to incorporate the topic of cognition to aid users in reflecting on what password creation strategies may work best for them. For those with low levels of need for cognition, training may be able to encourage users to spend more time thinking about each new password that they create. Encouraging the use of password managers may also be useful for these users.

Our results demonstrating a link between general risk-taking in daily life and password security behavior are consistent with prior research (Kennison & Chan-Tin, 2020). We found that men, but not women, who reported more daily risk-taking created weaker passwords for the new banking app. Higher levels of general risk-taking for women was related to being more likely to reuse the newly created password for the three new apps. For men, higher levels of risk-taking were related to being more likely to share passwords in the future. Our results showing that women reporting more frequent forgetting in daily life take more risks in daily life is novel and worthy of future research. It is unclear whether memory problems contribute directly to taking risks or whether there is a third variable affecting memory and risk-taking.

Our results showed that individuals with lower cyber security knowledge created weaker passwords. Lower cyber security knowledge was also related to greater likelihood of re-using passwords in the future. Both of these findings are consistent with prior research, showing that individuals with more cyber security knowledge are less likely to engage in risky cyber security behavior (Kennison & Chan-Tin, 2020; McCrohan et al., 2010; Peker et al., 2016). The fact that individuals with high levels of password security knowledge may choose to use weak passwords for some apps is especially risky if they re-use the weak password or a variant of it for other apps in the future. For example, previous research has shown that cracking a weak password for one user's account can lead to cracking the stronger passwords for the same user (Haque et al., 2013).

The results have implications for the development of theories describing the cognitive processes involved in creating passwords for different kinds of account. Few prior studies of cybersecurity behavior have utilized models of cognitive processes, which incorporate multiple stages of planning and individual differences factors. The lack of theory development including psychological variables on this topic is due, at least in part, to the fact that the work in the area is most often carried out by researchers with backgrounds in computer science rather than in psychology or other social sciences. Most prior research has been geared towards the creation of cybersecurity education programs or trainings and

identifying individuals most in need of training based on their personality traits (Alohali et al., 2018; Kennison & Chan-Tin, 2020; Kennison et al., 2021; Russell et al., 2017; Shappie et al., 2019), but has paid limited attention to cognitive processing and/or motivation. Few studies have examined the process of planned cybersecurity behavior as a process that could be approached as a process model (e.g., Camp et al., 2016), which could be used to frame future empirical investigations. We hope the present research serves to call attention to the need for more detailed theoretical approaches to cybersecurity behaviors. The present results show the importance of incorporating individual differences in need for cognition and everyday memory failures in future models. Future research may aim to focus on different aspects of memory ability, such as working memory capacity, memory for past events (i.e., retrospective memory), and memory for tasks to be completed in the future (i.e., prospective memory).

Most of the research has focused on recommendations for cybersecurity training (Aldawood & Skinner, 2019; McCrohan et al., 2010; Peker et al., 2016; Taylor-Jackson et al., 2020). Our results inform these endeavors as well. For those with the most severe everyday memory failures, they could be encouraged to learn about and consider adopting a password manager, which can be used to create a strong unique password for every account. Prior research by Kennison and Chan-Tin (2021) showed that only about a third of college students know what passwords managers are. Those individuals who may have relatively low levels of need for cognition could be encouraged to spend more time thinking about cybersecurity generally, and strategies to create strong passwords, specifically. Future research is needed to estimate the optimal amount of time that one should spend when creating a new password and engaging in effort to remember that password.

The research has multiple limitations. Foremost, we analyzed self-reported responses collected in an online survey. It is unclear whether passwords created in research studies are comparable to the passwords users create in daily life. Future research may be able to develop better methods for asking participants about their password security behavior. For participants who frequently re-use passwords in daily life, they may be especially unwilling to respond to survey questions in which they are asked to generate new passwords for hypothetical contexts. Second, our sample of college students was drawn from a psychology department in a relatively inexpensive public university located in the central region of the United States. Participants were young adults who were on average 20 years old and predominantly White. The ratio of women to men in the sample was approximately 3:1. It is possible that future research with samples of college students drawn from different types of institutions and

academic departments and with a better gender balance may observe different results.

In summary, the research showed that when creating new passwords, users create stronger passwords for some types of apps (i.e., banking app and email app) versus others (i.e., social media app). The results also showed that individual differences in everyday memory failures and need for cognition, a personality trait reflecting motivation to engage in mental activity, predicted password strength. Those reporting more everyday memory failures and those reporting the lowest levels of need for cognition were more likely to create weak passwords. Future training programs to raise awareness about password security could include self-assessments of everyday memory problems and need for cognition in addition to information about the characteristics of strong passwords. The research supports the view that the there is a need for theories of planned cybersecurity behavior that incorporates multiple stages of processing and individual difference factors (e.g., gender, personality, and cognitive factors, such as memory ability).

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46. https://doi.org/10.1145/322796.322806

Afifi-Sabet, K. (2021). SolarWinds blames intern for weak 'solarwinds123' password. Retrieved June 19, 2022 from https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs - pitfalls and ongoing issues. *Future Internet 11*, 73. https://doi.org/10.3390/fi11030073

Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia university students. *International Journal of Advanced Computer Science and Applications, 12*(3).

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

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), 2589. https://doi.org/10.3390/app12052589

Al-Zahrani, A. (2015). Toward digital citizenship: examining factors affecting participation and involvement in the internet society among higher education students. *International Education Studies, 8*(12), 203-217. http://dx.doi.org/10.5539/ies.v8n12p203

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Ba, M. H. N., Bennett, J., Gallagher, M., & Bhunia, S. (2021, December). A case study of credential stuffing attack: Canva data breach. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 735-740. https://doi.org/ 10.1109/CSCI54926.2021.00187

Bada, M., Sasse, A.M., Nurse, J.R.C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? In International Conference on Cyber Security for Sustainable Society, CSSS, 118–131. https://doi.org/10.48550/arXiv.1901.02672

Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology, 42*(1), 116. https://doi.org/10.1037/0022-3514.42.1.116

Cacioppo, J. T., Petty, R. E., & Feng Kao, C. (1984). The efficient assessment of need for cognition. *Journal of Personality Assessment, 48*(3), 306-307. https://doi.org/10.1207/s15327752jpa4803_13

Cacioppo, J. T. Petty, R. E., & Sidera, J. (1982). The effects of a salient self-schema on the evaluation of a pro-attitudinal editorial: Top-down versus bottom-up message processing. *Journal of Experimental Social Psychology, 18*, 324-338. https://doi.org/10.1016/0022-1031(82)90057-9

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. https://doi.org/10.1016/j.jisa.2018.08.002

Camp, L. J., Abbott, J., & Chen, S. (2016, January). Cpasswords: Leveraging episodic memory and human-centered design for better authentication. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 3656-3665. IEEE. https://doi.org/ 10.1109/HICSS.2016.457

Cluley, G. (2021). GoDaddy hack exposes accounts of 1.2 million customers. *Industry News.* Retrieved June 19, 2022 from https://www.bitdefender.com/blog/hotforsecurity/godaddy-hack-exposes-accounts-of-1-2-million-customers/

Cordova, J., Eaton, V., Greer, T., & Smith, L. (2017). A comparison of CS majors and non-CS majors attitudes regarding computer security threats. *Journal of Computing Sciences in Colleges, 33*(2), 4-10.

Cotton, K., & Ricker, T. J. (2022). Examining the relationship between working memory consolidation and long-term consolidation. *Psychonomic Bulletin & Review*, 1-24. https://doi.org/10.3758/s13423-022-02084-2

Debb, S. M., & McClellan, M. K. (2021). Keeping the human in the loop: Awareness and recognition of cybersecurity within cyberpsychology. *Cyberpsychology, Behavior, and Social Networking, 24*(9), 581-583. https://doi.org/ 10.1089/cyber.2021.0043

Dunaway, M., & Macharia, M. (2021). The effect of digital citizenship on negative online behaviors and learning outcomes in higher education. *Journal of Information Systems Education, 32*(4).

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*. https://doi.org/10.1002/sec.1184.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*

(WWW '07). Association for Computing Machinery, New York, NY, USA, 657–666. https://doi.org/10.1145/1242572.1242661

Fleischhauer, M., Enge, S., Brocke, B., Ullrich, J., Strobel, A., & Strobel, A. (2009). Same or different? Clarifying the relationship of need for cognition to personality and intelligence. *Personality and Social Psychology Bulletin, 36*(1): 82–96. doi:10.1177/0146167209351886

Forsberg, A., Guitard, D., & Cowan, N. (2021). Working memory limits severely constrain long-term retention. *Psychonomic Bulletin & Review, 28*(2), 537-547. https://doi.org/10.3758/s13423-020-01847-z

Gao, X., Yang, Y., Liu, C., Mitropoulos, C., Lindqvist, J., & Oulasvirta, A. (2018). Forgetting of passwords: Ecological theory and data. 27th USENIX Security Symposium (USENIX Security 18), 221-238.

Gärtner, A., Grass, J., Wolff, M., Goschke, T., Strobel, A., & Strobel, A. (2021). No relation of need for cognition to basic executive functions. *Journal of Personality, 89*(6), 1113-1125. https://doi.org/10.1111/jopy.12639

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R., Regenscheid, A., Burr, W. E., Richer, J. P., Lefkovitz, N., Danker, J. M., Choong, Y.-Y., Greene, K. K. & Theofanos, M. (2020). Digital identity guidelines: Authentication and lifecycle management. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-63b

Gratian, M, Bandi, S, Cukier, M, Dykstra, J, & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computer Security, 73*, 345 – 358. https://doi.org/10.1016/j.cose.2017.11.015

Haque, S.M. T., Wright, M., & Shannon Scielzo. (2013). A study of user password strategy for multiple accounts. *In Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13)*. Association for Computing Machinery, New York, NY, USA, 173–176. https://doi.org/10.1145/2435349.2435373

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. In R. Deng, V. Gauthier-Umaña., M. Ochoa, & M. Yung (Eds) *Applied Cryptography and Network Security. ACNS 2019. Lecture Notes in Computer Science* (pp. 217-237). Springer, Cham. https://doi.org/10.1007/978-3-030-21568-2_11

IBM. (2021). Cost of a data breach report 2021. Retrieved June 17, 2022 from https://www.ibm.com/downloads/cas/OJDVQGRY

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., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails? *Computers in Human Behavior Reports*. https://doi.org/10.1016/j.chbr.2021.100132

Lorenz, B., Kikkas, K., & Klooster, A. (2013, July). The four most-used passwords are love, sex, secret, and god: Password security and training in different user groups. In International Conference on Human Aspects of Information Security, Privacy, and Trust. In L. Marinos & I. Askoxylakis (Eds). *Human Aspects of Information Security, Privacy, and Trust. HAS*

2013. Lecture Notes in Computer Science (pp. 276-283), *8030*. Springer. https://doi.org/10.1007/978-3-642-39345-7_29

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce, 9*(1), 23-41. https://doi.org/ oi:10.1080/15332861.2010.487415

Meyer, B. (2022). Most common passwords: latest 2022 statistics. Cybernews. Retrieved June 20, 2022 from https://cybernews.com/best-password-managers/most-common-passwords/

Montejo Carrasco, P. M., Peña, M. M., & Sueiro, M. J. (2012). The memory failures of everyday questionnaire (MFE): internal consistency and reliability. *The Spanish Journal of Psychology, 15*(2), 768-776. https://doi.org/10.5209/rev_SJOP.2012.v15.n2.38888

O'Flaherty, K. (2019, October 20). Equifax lawsuit: 'Admin' as password at time of 2017 breach. https://www.forbes.com/sites/kateoflahertyuk/2019/10/20/equifax-lawsuit-reveals-terrible-security-practices-at-time-of-2017-breach/?sh=10bd50563d38

Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education, 26*(4), 281-294. https://jise.org/Volume26/n4/JISEv26n4p281.html

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016, October). Raising Cybersecurity Awareness among College Students. *Journal of the Colloquium for Information System Security Education, 4*(1), 1-17. https://par.nsf.gov/servlets/purl/10206543

Pilar, D. R., Jaeger, A., Gomes, C. F., & Stein, L. M. (2012). Passwords usage and human memory limitations: A survey across age and educational background. *Plos One, 7*(12), e51067. https://doi.org/10.1371/journal.pone.0051067

Plachkinova, M., & Maurer, C. (2019) Security breach at Target. *Journal of Information Systems Education, 29*(1), Article 7. https://aisel.aisnet.org/jise/vol29/iss1/7

Ponemon Institute. (2019). Cost of a data breach 2019. Retrieved June 19, 2022 from https://www.ibm.com/downloads/cas/RDEQK07R.

Ponemon Institute. (2021). Cost of a data breach 2019. Retrieved June 19, 2022 from https://www.ibm.com/security/data-breach

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

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. The *Journal of Psychology, 91*, 93–114. https://doi.org/10.1080/00223980.1975.9915803

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

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture*, 9(4), 475 – 480. https://doi.org/10.1037/ppm0000247

Sunderland, A., Harris, J. E., & Baddeley, A. (1983). Do laboratory tests predict everyday memory? A neuropsychological study. *Journal of Verbal Learning and Verbal Behaviour, 22*, 341–357. http://dx.doi.org/10.1016/S0022-5371(83)90229-3

Taylor-Jackson, J., McAlaney, J., Foster, J., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education: A pedagogical approach. Proceedings of Asia USEC'20, Financial Cryptography and Data Security (pp. 207 – 217). https://doi.org/10.1007/978-3-030-54455-3_15

Tick, A., Cranfield, D. J., Venter, I. M., Renaud, K. V., & Blignaut, R. J. (2021). Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics, 10*(22), 2865. https://doi.org/10.3390/electronics10222865

Veroni, E., Ntantogian, C., & Xenakis, C. (2022). A large-scale analysis of Wi-Fi passwords. *Journal of Information Security and Applications, 67*, 103190. https://doi.org/10.1016/j.jisa.2022.103190

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757. https://doi.org/10.1016/j.ijhcs.2007.03.007

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems, 19*(3). https://doi.org/10.48009/3_iis_2018_150-159

Wheeler, D.L. (2016). Zxcvbn: Low-budget password strength estimation. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, pp. 157–173

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, 111, 36-48. https://doi.org/10.1016/j.ijhcs.2017.11.002

Xu, S., Yang, H., & Zhu, S. (2019). An investigation of 21st-century digital skills on digital citizenship among college students. 2019 International Symposium on Educational Technology (ISET) (pp. 236-240). IEEE. https://doi.org/10.1109/ISET.2019.00056.

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior, 121,* 106791. https://doi.org/10.1016/j.chb.2021.106791

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

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems, 62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Authors' Note:
Funding: This work was supported by the National Science Foundation [grant numbers DGE 1918591, DGE 1919004]. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The data reported in this manuscript are available upon reasonable request from the corresponding author.