Computers in Human Behavior Reports 4 (2021) 100132

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

Who creates strong passwords when nudging fails

Shelia M. Kennison [a,*], Ian T. Jones [a], Victoria H. Spooner [a], D. Eric Chan-Tin [b]

[a] Oklahoma State University, USA
[b] University of Loyola Chicago, USA

ARTICLE INFO

Keywords:
Cybersecurity
Secure passwords
Personality traits
Nudging
Risk-taking
Self-schemas

ABSTRACT

The use of strong passwords is viewed as a recommended cybersecurity practice, as the hacking of weak passwords led to major cybersecurity breaches. The present research investigated whether nudging with messages based on participants' self-schemas could lead them to create stronger passwords. We modeled our study on prior health-related research demonstrating positive results using messages based on self-schema categories (i.e., True Colors categories -compassionate, loyal, intellectual, and adventurous). We carried out an online study, one with 256 (185 women, 66 men, 5 other) undergraduates and one with 424 (240 men, 179 women, 5 other) Amazon Mechanical Turk (MTurk) workers, in which we randomly assigned participants to receive messages that matched or mismatched their self-schema. We also investigated whether differences across the Big Five personality traits, secure password knowledge, attitudes and behavior, need for cognition, and general risk-taking predicted the strength of passwords that participants created during the study. Multiple individual difference variables predicted password strength (i.e., conscientiousness, emotional stability, need for cognition, self-reported secure password knowledge, attitude, and behavior, and general risk-taking). MTurk workers had higher levels of cybersecurity knowledge and created stronger passwords than college students. The nudging messages did not lead to stronger passwords. Implications for strategies to increase the use of secure passwords are discussed.

Cybersecurity threats continue to be a major concern for individuals and institutions around the world (Singer & Friedman, 2014). The use of weak passwords has contributed to some high-profile cybersecurity breaches, including those at Target (Plachkinova & Maurer, 2019) and Equifax (O'Flaherty, 2019; Wang & Johnson, 2018). An investigation by Verizon in 2017 indicated that 81 percent of corporate security breaches were due to weak passwords being hacked (Verizon, 2017). Efforts to increase cybersecurity in organizations has included the use of educational training (Bryant & Campbell, 2006; Ferguson, 2005; McCrohan et al., 2010; Peker et al., 2016; Taylor-Jackson et al., 2020; See Proctor, 2016, for review). Training is a reasonable approach, as surveys have shown that awareness about cybersecurity issues is low among members of the general public in the United States, even among those who have been affected by a cybersecurity breach (Pew Research Center, 2017). Nevertheless, some research has shown that training is ineffective (Bada et al., 2019; Ferguson, 2005; Lorenz et al., 2013; Notoatmodjo & Thomborson, 2009; Riley, 2006). Recent research has explored the use of nudges (i.e., indirect suggestion) to improve cybersecurity practices (Guo et al., 2020; Li, 2016; Peer et al., 2020; Renaud & Zimmermann, 2019; Seitz et al., 2016). The aim of the present research was to investigate whether nudging messages may increase the likelihood that adults create strong passwords and the factors related to strong password practices.

Breaches in cybersecurity can occur when a weak password has been guessed by hackers who may use computer algorithms designed for that purpose (Farcasin & Chan-Tin, 2015; Hitaj et al., 2019; Houshmand et al., 2015; Ji et al., 2015; Narayanan & Shmatikov, 2005; Melicher et al., 2016; Tatlı, 2015; Weir et al., 2009; Zhang et al., 2020). One of the major breaches in 2017 involved the credit reporting agency Equifax (O'Flaherty, 2019). An investigation into the cause of the breach revealed that a weak password (i.e. admin) made it susceptible to hacking. Research has suggested that using weak passwords is among the most common risky cybersecurity behaviors (Florencio & Herley, 2007; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). Strong passwords are those that are not easily guessed, and weak ones are those that can be guessed with or without password hacking software. In prior research, the strength of a password has been assessed in multiple ways. Some researchers have used algorithms to guess the password with the

* Corresponding author.
E-mail address: shelia.kennison@okstate.edu (S.M. Kennison).

https://doi.org/10.1016/j.chbr.2021.100132
Received 5 March 2021; Received in revised form 7 August 2021; Accepted 8 August 2021
Available online 13 August 2021
2451-9588/Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

programs providing a strength score (Das et al., 2014; Farcasin & Chan-Tin, 2015; Golla; Durmuth, 2018; Guo et al., 2020; Kelley et al., 2012). Other researchers have generated strength scores for passwords based on the types of characters in the passwords with combinations of numbers, uppercase letters, lower case letters, and special symbols receiving higher strength scores (e.g., Pittman & Robinson, 2020 , December).

Organizations frequently use cybersecurity training as a way of raising awareness about cybersecurity best practices, including the importance of using strong passwords (Adams & Sasse, 1999; Aldawood & Skinner, 2019; Bryant & Campbell, 2006; Ferguson, 2005; McCrohan et al., 2010; Peker et al., 2016; Taylor-Jackson et al., 2020; For review see Proctor, 2016). Adams and Sasse (1999) have claimed that some institutions may not use adequate communications with their members about cybersecurity risks and what practices are risky. Some studies have observed positive outcomes following training about best practices and specific cybersecurity threats (McCrohan et al., 2010; Peker et al., 2016). There are a growing number of studies that document the relationship between higher levels of cybersecurity knowledge and a lower likelihood of engaging in risky cybersecurity behavior (Ferguson, 2005; Kennison & Chan-Tin, 2020; McCrohan et al., 2010; Peker et al., 2016). Other studies have found cybersecurity training to have limited benefits (Bada et al., 2019; Ferguson, 2005; Lorenz et al., 2013; Notoatmodjo & Thomborson, 2009; Riley, 2006). Studies have found that participants will engage in a risky cybersecurity behavior (e.g., using a weak password) even when they know that it is risky (Notoatmodjo & Thomborson, 2009; Riley, 2006). Cybersecurity researchers recognize that there is need for new approaches to reduce people's likelihood of taking risks with cybersecurity (See Corradini, 2020; for review).

Prior research has found that there are differences across groups in cybersecurity knowledge (Anwar et al., 2017; Cain et al., 2018; Gratian et al., 2018; Kennison & Chan-Tin, 2020; McCormac et al., 2017; Whitty et al., 2015). For example, studies have shown that cybersecurity knowledge can be higher for men than for women (Cain et al., 2018; Kennison & Chan-Tin, 2020) and that men report engaging in risky cybersecurity behavior more often than women (Anwar et al., 2017; Gratian et al., 2018). Other studies have shown that older adults may be less knowledgeable of cybersecurity issues than young adults (Gratian et al., 2018); however, in studies of cybersecurity behavior, significant differences related to age have not been observed (Cain et al., 2018; Grimes et al., 2010; McCormac et al., 2017; Whitty et al., 2015).

Many studies have explored the extent to which cybersecurity behaviors can be predicted by Big five personality traits, which include conscientiousness, extraversion, agreeableness, openness, and emotional stability (Alohali et al., 2018; Kennison & Chan-Tin, 2020; Maraj et al., 2019; McBride et al., 2012; McCormac et al., 2017; Russell et al., 2017; Shappie et al., 2019; Tamrakar et al., 2016). Multiple studies have found that lower levels of conscientiousness are related to higher levels of risky cybersecurity behavior (Alohali et al., 2018; Kennison & Chan-Tin, 2020; Russell et al., 2017; Shappie et al., 2019). A few studies have found that lower levels of emotional stability are related to higher levels of risky cybersecurity behavior (Kennison & Chan-Tin, 2020; Shappie et al., 2019).

Kennison and Chan-Tin (2020) found that a combination of personal characteristics, including gender, conscientiousness, emotional stability, self-reported knowledge about cybersecurity issues, and general risk-taking unrelated to cybersecurity accounted for 34 percent of the variance in self-reported cyber security behaviors. Those reporting higher levels of general risk-taking reported higher levels of risky cybersecurity behaviors. They measured risk-taking for five general domains: social, health/safety, financial, ethical, and recreational. These results are consistent with the view that people who more often engage in one category of risk-taking may be more likely to carry out other types of risk-taking than others (Kennison et al., 2016; Shou & Olney, 2020). Research on general risk-taking has shown that men tend to take more risks than women (Gustafsod, 1998; Kennison et al., 2016; Kennison et al., 2016; Weber et al., 2002; See Panno et al., 2018 for review).

A growing number of researchers are taking a new approach to cybersecurity, which involves using nudges, which refers to indirect suggestions to influence behavior, to increase the use of secure behaviors (Egelman et al., 2013; Guo et al., 2020; Kankane et al., 2018; Peer et al., 2020; Renaud & Zimmermann, 2019; Vance et al., 2013). Thaler and Sunstein (2009) first described nudging as a method of influencing choice behavior (c.f., Hansen, 2015). Since then, researchers have investigated the effectiveness of nudging to influence a wide variety of behaviors (Halpern, 2015). However, some researchers have found nudging to be ineffective (Rayner & Lang, 2011). In recent years, there have been several studies investigating whether nudging can affect cybersecurity behaviors, including the use of stronger passwords (Egelman et al., 2013; Guo et al., 2020; Renaud & Zimmermann, 2019; Vance et al., 2013). In a series of studies, Renaud and Zimmermann (2019) tested the effectiveness of nudges design to strengthen users' passwords. In the first two studies, eight visual nudges were tested ranging from simple text (e.g., *choose a password* and *choose a secret)* to simple images that indicate the password strength compared with others at the organization to images displaying the password strength along a continuum from weak to strong. None of these simple nudges produced meaningful changes in password strength. Their only success in nudging participants to use stronger passwords was their third study in which they tested a hybrid nudge involving three elements: a visual nudge (i.e., a cartoon with the message *The stronger your password, the longer you can use it.)*, a nudging reminder (i.e, a prominent display of the password's expiration, users' last login date and clickable button to change password), an incentive to the user to create a strong password (i.e., as participants typed in their password, the password's strength dynamically changed its expiration date). Renaud and Zimmermann (2019) concluded that in order for password nudges to be effective they *must contain clear and unambiguous information about the benefits of strong passwords.*

In the present study, we investigated whether nudging could lead adults to create strong passwords and the factors related to strong password practices. We modeled our approach of using nudging messages on prior research supporting schema correspondence theory (Brannon & Brock, 2006), which claims that messages that are consistent with one's self-schema (i.e., how one thinks of oneself) can indirectly influence (or nudge) subsequent behaviors (Brannon & Brock, 1994; Brannon & McCabe, 2002, 2003; Brock et al., 1990; Miller & Brannon, 2015; Pease et al., 2006; Pilling & Brannon, 2007; York et al., 2012a; See also; Cacioppo et al., 1982). For example, Brannon and McCabe (2002) showed that there was greater impact of information contained in an AIDS prevention message when the message was matched to participants' self-schema. In addition, the results showed that participants who reported lower levels of need for cognition (i.e., the degree to which one enjoys thinking) were influenced by matching (versus mismatching messages) more than others. The approach of matching informational messages to self-schemas has been shown to influence other types of messages, including purchasing preferences (Brock et al., 1990), drinking alcohol (Pilling & Brannon, 2007; York et al., 2012a, 2012b), multiple health-related risk behaviors (Pease et al., 2006). In several studies by Brannon and colleagues (Brannon & Brock, 1994; Brannon & McCabe, 2002, 2003; Brock et al., 1990; Miller & Brannon, 2015; Pease et al., 2006; Pilling & Brannon, 2007; York et al., 2012a, 2012b), participants' self-schemas were one of four categories from the True Colors categories (e.g., blue-compassionate, gold-loyal, green-intellectual, and orange-adventurous) (Kiersey & Bates, 1978; Lowry, 1987; True Colors, 2021).

In our study, we asked participants to identify their self-schema category (i.e., which True Colors category is most like them). Subsequently, they were randomly assigned to receive a message that had been crafted to emphasize words related to their self-schema category or to receive a message developed for the category that they indicated was

least like them. Later, they were asked to create a password that they would use in the second session of the study, which would occur approximately one month later. We recruited participants from a university courses and MTurk, an online platform on which individuals can receive pay for completing surveys. We recognized that prior research has found that the personal characteristics of samples sometimes differ with samples recruited from MTurk with MTurk respondents tending to be older and tending to have higher levels of education (Paolacci et al., 2010; Ross et al., 2010) than samples drawn from the general population. Casler et al. (2013) also found that MTurk respondents were higher in socio-economic status and more ethnically diverse than respondents recruited via social media (See also Behrend et al., 2011). Redmiles et al. (2019) found that MTurk respondents had higher levels of cybersecurity knowledge than the general population.

We hypothesized that participants who received a message that matched their self-schema would create stronger passwords than those who received a mismatching message. We also investigated whether need for cognition (i.e., how much a person enjoys thinking generally, Cacioppo et al., 1984) would be related to how effectiveness schema-based nudges would be, as occurred in prior research (Brannon & McCabe, 2002). In addition, we hypothesized that MTurk participants would create stronger passwords than college students, as their levels of cybersecurity knowledge were expected to be higher than that of college students. We also examined whether password strength would be related to cybersecurity knowledge, Big Five personality traits (i.e., conscientiousness, neuroticism, agreeableness, openness, and extraversion), general risk-taking, and type of sample (i.e., MTurk vs. college students). We tested the additional hypotheses: a) those with higher levels of cybersecurity knowledge would create stronger passwords than others; b) higher levels of conscientiousness would be related to stronger passwords; c) higher levels of emotional stability would be related to stronger passwords; and d) higher levels of general risk-taking would be related to weaker passwords.

Method

Participants

Two samples of participants were collected for the current study, an undergraduate sample recruited from the local university and a sample of workers on Amazon's Mechanical Turk. The first included 256 (185 women, 66 men, 5 other) undergraduates with a mean age of 18.8 years (SD = 1.46, Min = 18, Max = 25) who received course credit in exchange for participation. The second included 424 (240 men, 179 women, 5 other) participants were workers on Amazon's Mechanical Turk with a mean age of 38.3 years (SD = 11.4, Min = 20, Max = 73) who received $2.00 for participation. The undergraduate sample was composed of the following ethnic groups: 74.6% White and 25.4% other or more than one category (5.1% Latinx/Hispanic, 4.3% Black, 3.9% Native American, 0.4% Asian, and 11.7% more than one category). The MTurk sample was composed of the following ethnic groups: 74.9% White and 25.1% other or more than one category (4.7% Latinx/Hispanic, 8.1% Black, 0.9% Native American, 7.6% Asian, and 3.8% more than one category).

Materials

We assessed participants' self-schemas using the True Colors categories (Keirsay & Bates, 1978; Lowry, 1987), following the procedure used previously by Brannon and colleagues (Brannon & Brock, 1994; Brannon & McCabe, 2002, 2006; Brock et al., 1990; Miller & Brannon, 2015; Pease et al., 2006; Pilling & Brannon, 2007; York et al., 2012a, 2012b). Participants were shown four images depicting the four categories, which were created in the 1970s as a way of categorizing people into four types (Keirsey & Bates, 1978; Lowry, 1987; for images, see Brock et al., 1990). Brannon and McCabe (2002) reported that the assessment using images was shown to have excellent test-retest reliability (i.e., participants' image choice were stable across two testing sessions). They indicated that the reliability of the measure was shown to be excellent in Brock et al. (1990). In the present study, participants were asked to select the image that was most like them (See Brock et al., 1990 for copies of the images). The instructions were as follows: *Which of the images above best describes you? (We realize that you may feel drawn to more than one image. Select the image that is MOST like you. Because the text in the images is small and hard to read, we have provided the text in the choices below.)*

Image A I am warm, communicative, compassionate, and feeling. I need to search for the meaning and significance of life. I want to find ways to make my life count and matter, to become my own authentic self. Integrity, harmony, and honesty are very important to me. I feel that I am highly idealistic and spiritual by nature.

Image B I need to be responsible, dependable, helpful, and sensible. I want to fulfill my duties and obligations, to organize and to structure my life as I see fit. I am practical, sensible, and punctual, and I believe that people should earn their way through work and service to others.

Image C I am versatile, wise, conceptual, and curious. I need freedom to pursue knowledge and wisdom to develop competency by acquiring skills and capabilities. I think life is something to make sense of, to be understood, and explained.

Image D I am adventurous, skillful, competitive, and spontaneous. I need to be free to act on a moments notice, impulsively and spontaneously. I believe that life is to enjoy, so I thrive on fun, variety, and excitement. Living in the moment, I act on every opportunity.

We constructed messages containing information about cybersecurity, which contained descriptive phrases that were consistent with each of the True Colors categories: blue-compassionate (Image A), gold-dependable (Image B), green-intellectual (Image C), and orange-adventurous (Image D) (e.g., Gold - *You are a responsible person and other people can depend on you.*). In each message, we incorporated multiple words shown to be related to the category (Kiersey & Bates, 1978; Lowry, 1987). These messages are displayed in Table 1.

We assessed need for cognition using Cacioppo and Petty's (1982) 18-item need for cognition scale. Participants indicated how well the statement described them using a 5-point scale (i.e., 1 = *Strongly Disagree*, 5 = *Strongly Agree*). We computed a mean, after reverse scoring some items, such that higher means indicated higher levels of need for cognition. Prior research has found the need for cognition scale to have adequate internal consistency (Cronbach alpha α = .90, Cacioppo et al., 1982; 1984). In the present research, we also observed high internal consistency (Cronbach α = .94).

We assessed participants' knowledge, attitudes, and behaviors related to using secure passwords using 9-items from the human aspects of information security questionnaire (HAIS-Q) (Parsons et al., 2017). Three items assessed knowledge (e.g., *It's acceptable to use my social media passwords on my work accounts.*); three items assessed attitude (e.g., *It's safe to have a work password with just letters.*), and three items assessed behaviors (e.g., I use a combination of letters, numbers, and symbols in my work passwords.). For each item, participants indicated their level of agreement using a 7-point scale (i.e., 1 = *Strongly Disagree*, 2 = Disagree, 3 = Slightly Disagree; 4 = Neither Disagree nor Agree; 5 = *Slightly Agree, 6 = Agree,* and *7 = Strongly Agree*). In prior research, the measure has been found to have high internal consistency (i.e., Cronbach alphas over α = .70, Parsons et al., 2017). In the present study, we also observed acceptable internal consistency only when the nine items were considered as a single factor (Cronbach alphas α = .72). We computed the mean rating for the nine items, after reverse scoring some items. Higher means reflecting higher levels of knowledge, attitudes,

Table 1
Summary of descriptive statistics.

Category	Message
Blue	You generally care about others, so you want to make sure that your friends or family accounts are not compromised. Using a weak and easily-guessable password means that hackers can get into your accounts. For example, if they get into your social media account, they might post messages to your family and friends pretending to be you. If the hackers are able to get into your family's banking account, they might steal their money which in turn, will cause grief to these family members. Be true to yourself and those you value, use a strong password!
Gold	You generally are a responsible person and other people can depend on you.Using a weak password means that hackers can easily guess your password and get into your account. This means they can then easily impersonate you or obtain sensitive information about your family and friends, such as birth dates, phone numbers, etc. You do not want to be irresponsible and let that kind of information fall into the hackers' hands as this could lead to identity theft and other forms of frauds. Be responsible, use a strong password!
Green	You generally are a knowledgeable and curious individual. You should feel challenged on how to create a good password that is not easily guessable by hackers. Using your knowledge and creativity, you can come up with good, strong passwords. You can then share that knowledge with your family and friends so that they do not get easily hacked. Learning good password creation, usage, and management will enhance your knowledge and is something new for you to learn and master. Be smart, use a strong password!
Orange	You generally want to show off your skills and win competitions. You do not want to be listed in the "hall of shame" by being an individual whose account has been hacked due to using a weak password. You want to win against the hackers and prevent them from controlling your life or your online accounts. By not using a weak password, you can show off with your friends and families that your accounts have not been hacked. You can even show them how to use a good password. Live an exciting life, use a strong password!

and behavior about secure password knowledge, attitude, and behaviors.

We assessed Big Five personality traits (i.e., openness, conscientiousness, agreeableness, extraversion, and neuroticism/emotional stability) using Saucier's (1994) mini-marker questionnaire, which includes eight adjectives per trait for a total of 40 adjectives. For each trait, participants indicated how well the adjective described them (i.e., 1=extremely inaccurate, 2 = *very inaccurate*, 3 = *moderately inaccurate*; 4 = *slightly inaccurate*; 5 = *neither accurate nor inaccurate*; 6 = *slightly accurate*; 7 = *moderately accurate*; 8 = *very accurate,* and 9=extremely accurate). We computed the mean rating per trait, after reverse scoring some items. In prior research, the measure has been found to have high internal consistency (i.e., Cronbach alphas between .77 and .92, Thompson et al., 2021, in press). In the present study, we also observed high internal consistency (Cronbach alphas between α = .76 and α = .87).

We assessed general risk-taking not related to cybersecurity behaviors using Blais and Weber's (2001; 2006) Domain-Specific Risk-Taking Attitude Scale (DOSPERT), which distinguished five domains of risk-taking (i.e., health, financial, ethical, social, and recreational). For each domain, there are six items describing risky behaviors. Participants were asked to indicate how likely they were to participate in the behavior on a 7-point scale (i.e., *1 = Extremely Unlikely, 2 = Moderately Unlikely, 3 = Somewhat Unlikely; 4 = Neither Unlikely nor Likely; 5 = Somewhat Likely; 6 = Moderately Likely,* and *7 = Extremely Likely*). We computed the mean rating for each domain, with higher means reflecting higher levels of likelihood to engage in that type of risk. Prior research has found the DOSPERT to have adequate internal consistency (Cronbach alphas between α = .71 and α = .84, Frey et al., 2017; Kennison et al., 2016). In the present research, we also observed adequate internal consistency (Cronbach alphas between α = .73 and α = .86).

We assessed gender with a question in which participants selected one of the following categories: a) *man*; b) *woman*; c) *transgender*; d) *gender non-conforming/non binary*; and e) *I identify with a gender not listed*.

We asked participants to create a password with a minimum of eight characters, which they would use in a second session for the study. Participants entered the password into a textbox in the survey.

We also included a question in the survey 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*.

Procedures

We obtained approval for the research from the Institutional Review Board prior to recruitment. For our sample of undergraduates, we recruited volunteers on a SONA research pool in a Psychology Department. For the MTurk sample, we recruited workers residing in the United States. All participant received the questions in the same order: questions about current devices, social media use, secure password knowledge, attitude, and behavior, Big Five personality, self-schema categories, need for cognition, evaluation of the messages, and new password creation.

We developed a scoring rubric to quantify password strength. We noted that many platforms now require passwords to contain specific characters. Our scoring system awarded 1-point if the password included each of the following characteristics (i.e., number, lowercase characters, uppercase characters, and special symbols). Passwords that did not contain any letter sequences that formed words or names received an additional point. Prior research has suggested that some security breaches occurred when passwords used dictionary words (Farcasin & Chan-Tin, 2015). The maximum strength score for a password as 5 and the minimum strength score, 1.

Results

Participants who responded incorrectly to the attention-check question were excluded from the data analyses (i.e., 32 from the SONA sample and 20 from the MTurk sample). Participants' responses were then used to compute mean password strength, which was normally distributed. We tested the hypothesis that participants would create stronger passwords following messages that matched their personality than following messages that mismatched their personality by conducting an analysis of variance (ANOVA). Mean password strength was the dependent variable, and the three between-participants independent variables were a) type of message with two levels (i.e., matching vs. mismatching), b) participants' self-schema category with four levels (i.e., blue, green, gold, and orange), and c) type of sample with two levels (i.e., SONA participant vs. MTurk participant). Need for cognition was entered as a covariate. The results did not support the hypothesis. Overall, passwords were stronger if participants had received a message that mismatched their self-schema: mismatching mean: 3.14 (SD = 1.32) vs. matching mean: 2.50 (SD = 1.26), $F(1,593) = 3.73$, $p = .052$. Using G-Power 3.1.9.7 (Faul & Erdfelder, 1992; Faul et al., 2007), we confirmed that for an effect size $d = .50$ with sample size $n = 425$ and alpha = .05, power was .95. The results supported the hypothesis that MTurk participants would create stronger passwords than SONA participants (3.38 vs 2.06), $F(1,593) = 41.32$, $p < .001$ and also had higher levels of cybersecurity knowledge than SONA participants, (6.05 vs 5.36), $F(1,514) = 8.10$, $p < .001$. We also found that those with higher levels of need for cognition created stronger passwords than others, $F(1,593) = 17.13$, $p < .001$. The remaining non-significant results include: a) the main effect of participants' self-schema was not significant, $F(3,593) = 1.27$, $p = .28$; b) the type of message x self-schema category interaction, $F(3,593) = .65$, $p = .58$. No other significant results were observed.

To test the remaining hypotheses, we computed mean scores for the

following variables: big five personality traits (conscientiousness, openness, extraversion, agreeableness, neuroticism), and secure password knowledge, attitude, and behaviors (i.e., HAIS-Q), and conducted analyses to investigate the extent to which participants' personal characteristics predicted password strength. Pearson's *r* moment-by-moment correlations were carried out for password strength and the variables. Table 2 displays these results with other descriptive statistics. The results supported the third hypothesis that those reporting higher levels of self-reported secure password knowledge, attitude, and behavior (as measured by the HAIS-Q) would create stronger passwords (men: $r = .40$, $p < .001$ and women: $r = .39$, $p < .001$). The results also supported the hypothesis that higher levels of conscientiousness would be related to stronger passwords (men: $r = .21$, $p < .001$ and women: $r = .20$, $p < .001$. The results also supported the hypothesis that higher levels of emotional stability would be related to stronger passwords (men: $r = .28$, $p < .001$ and women: $r = .15$, $p < .001$). The results also supported the hypothesis that participants with lower levels of general risk-taking in daily life would be related to stronger passwords (men: $r = -0.14$, $p = .02$ and women: $r = -0.11$, $p = .04$). There were additional results that were not addressed in our hypotheses. Participants with higher levels of openness created stronger passwords (men: $r = .23$, $p < .001$ and women: $r = .30$, $p < .001$). Participants with higher levels of agreeableness created stronger passwords (men: $r = .18$, $p = .003$ and women: $r = .11$, $p = .046$).

To explore further the extent to which the different variables predict password strength, we conducted a hierarchical multiple regression in which password strength was the dependent variable and the nine variables were entered as predictor variables. In Block 1, we entered gender and need for cognition. In Block two, we entered the Big Five variables. In Block 3, we entered general risk-taking and self-reported password knowledge, attitude, and behavior. Our rationale for how the blocks were order was that those personal characteristics that are highly stable across the lifespan were entered before variables that were less stable with those variables that are most likely to be influenced by life experiences being entered last. For the majority of individuals, gender identity develops in early childhood (Li et al., 2017). Need for cognition has been found to be related to fluid intelligence (Hill et al., 2013) for which genetics accounts for approximately 52% of individual variation (Nikolašević et al., 2021). Research has suggested that the approximately 50% of variation in Big Five personality traits are determined by genetics (Bouchard & Loehlin, 2001). They have been found to be stable across the lifespan (Conley, 1985), and some have suggested that they are universal (Yamagata et al., 2006). Recent research exploring the role of genetics in risk-taking found that only about 1.6% in the variation in risk-taking was due to genetics (Linnér et al., 2019). In our analysis, we observed acceptable Tolerance and VIF values (Coakes, 2005). A summary of the results is provided in Table 2. In Block 1, gender and need for cognition accounted for 7% of the variance in password strength, $F(2, 612) = 21.53$, $p < .001$. Both variables were significant predictors: gender ($\beta = .09$, $p = .028$) and need for cognition ($\beta = .23$, $p < .001$). In Block 2, the Big Five personality traits accounted for an additional 8% of variance in password strength, $F(7, 607) = 14.93$, $p < .001$ and the change in R^2 was significant, $F(7, 607) = 11.54$, $p < .001$. Three of the five traits were significant predictors: emotional stability ($\beta = .15$, $p = .001$), openness ($\beta = .17$, $p < .001$), and extraversion ($\beta = -0.19$, $p < .001$). In Block 3, general risk-taking and self-reported password knowledge, attitudes, and behavior accounted for an additional seven percent of the variance in password strength, $F(9, 605) = 18.55$, $p < .001$ and the change in R^2 was significant, $F(2, 605) = 26.79$, $p < .001$. Only self-reported password knowledge, attitude, and behavior was a significant predictor ($\beta = .31$, $p < .001$). Overall, the analysis showed that the variables accounted for 21 percent of the variance.

Table 3
Summary of hierarchical regression analysis for variables predicting password strength.

Variable	β	t	sr^2	R	R^2	ΔR^2
Block 1				.26	.07	.07***
Gender				.09	2.20*	.008
Need for Cognition		.23	5.86***	.05		
Block 2				.38	.14	.08***
Gender				.07	1.66	.003
Need for Cognition		.10	2.29*	.008		
Conscientiousness		.08	1.17	.004		
Emotional Stability		.15	3.24***.014			
Agreeableness			.02	.38	.000	
Openness			.17	3.63***	.020	
Extraversion			-.19	4.84***	.033	
Block 3				.47	.21	.07***
Gender				.07	−1.73	.004
Need for Cognition		.07	1.54	.003		
Conscientiousness		.01	.24	.000		
Emotional Stability		.09	2.05*	.000		
Agreeableness			-.002	-.03	.000	
Openness			.15	3.30	.014	
Table 3 cont'd						
Extraversion			-.13		−3.39***.015	
General Risk-Taking			.03		.77.000	
Password HAIS-Q			.31		7.27***.07	

Note. *p < .05, **p < .01, ***p < .001.

General discussion

We investigated whether adults could be nudged to create stronger passwords. The nudges were messages constructed to be consistent or inconsistent with participants' self-schemas (i.e., True Colors categories – compassionate, loyal, intellectual, and adventurous). We tested the hypothesis that participants would create stronger passwords after viewing a message that matched their self-schema than after viewing a mismatching message. The results did not support the hypothesis. The analysis showed that those higher in need for cognition created stronger

Table 2
Summary of correlational results.

Variable	1	2	3	4	5	6	7	8	9	Mean	SD
1. Password Strength	–	.39***	.20***	.15**	-.14*	.11*	.30***	.20***	-.11*	2.81	1.30
2. Password HAIS-Q	.40***	–	.35***	.27***	-.13*	.28***	.24***	.19***	-.19***	5.74	0.98
3. Conscientiousness	.21***	.40***	–	.39***	.13*	-.39***	.33***	.24***	-.33***	6.89	1.25
4. Emotional Stability	.28***	.40***	.50***	–	.27***	.42***	.21***	.19	-.21***	4.20	1.62
5. Extraversion	-.04	.01	.28***	.19**	–	.17**	.00	.02	.05	5.34	1.78
6. Agreeableness	.18**	.23***	.44***	.44***	.31***	–	.30***	.15**	-.28***	7.21	1.31
7. Openness	.23***	.27***	.42***	.24***	.36***	.37***	–	.47	-.19**	6.31	1.14
8. Need for Cognition	.27***	.33***	.33***	.34***	.28***	.19**	.60***	–	-.11	3.33	0.88
9. General Risk-Taking	-.14*	-.38***	-.27***	-.38***	-.01	-.26***	-.13*	-.11	–	102.01	23.13
Mean	3.12	5.78	6.74	3.71	5.20	6.78	6.49	3.50	110.12		
SD	1.35	1.10	1.34	1.46	1.76	1.41	1.31	0.85	30.21		

Note. Lower half of the matrix provides results for men and upper half provides results for women. *$p < .05$, **$p < .01$, ***$p < .001$.

passwords than others. We confirmed the hypothesis that MTurk participants created stronger passwords than SONA participants and also had higher levels of cybersecurity knowledge. The results also supported four additional hypotheses: a) higher levels of conscientiousness were related to stronger passwords; b) higher levels of emotional stability were related to stronger passwords; c) higher levels of self-reported secure password knowledge, attitude, and behavior were related to stronger passwords; and d) higher levels of general risk-taking were related to weaker passwords. In a hierarchical multiple regression analysis, we found that 21% of variance in password strength was accounted for by variables related to personality and other personal characteristics (e.g., general risk-taking and knowledge, attitude, and behavior related to passwords).

Prior studies have also found that nudging people to create stronger passwords may not work (Renaud et al., 2020). Nevertheless, we speculate that nudging could work if the content of our messages could be improved, such that they have a stronger impact on participants. In future research, it may also be useful to investigate whether the nudging effects of the messages could be increased if, prior to viewing the message, participants were explicitly told the message has been personalized for them using information about their self-schemas. Participants may be more likely to be affected by message content if they are told explicitly that the message has been tailored to them based on some personal characteristic (See Li, 2016 for discussion). In future studies in which personalized messages are created to nudge participants to create strong passwords, we anticipate that matching could be done using other characteristics, such as Big Five personality traits or other personality dimensions (e.g., honesty-humility).

Our research showing that those with higher levels of self-reported knowledge, attitude, and behavior about secure passwords created stronger passwords is consistent with prior research showing that those with more cybersecurity knowledge behave in ways more consistent with safe cybersecurity practices (Ferguson, 2005; Kennison & Chan-Tin, 2020; McCrohan et al., 2010; Peker et al., 2016). Our results showing that Big Five personality traits predicted participants' password strength are consistent with prior research (Alohali et al., 2018; Kennison & Chan-Tin, 2020; McBride et al., 2012; McCormac et al., 2017; Russell et al., 2017; Shappie et al., 2019; Tamrakar et al., 2016). We observed relationships between password strength and four of the five traits (i.e., conscientiousness, emotional stability, agreeableness, and openness). Higher levels of conscientiousness, agreeableness and openness predicted stronger passwords; higher levels of emotional stability predicted strong passwords. Our results showing that variables related to personality and other personal characteristics can be used to predict password strength make a unique contribution to the literature, as no prior study has shown that there is a link between general risk-taking in daily life and the strength of passwords. This result is consistent with recent research by Kennison and Chan-Tin (2020), which found that general risk-taking unrelated to cybersecurity predicted participants' self-reported risky cybersecurity behaviors. Information about who may be more likely to use weak passwords could be useful to organizations, as they may use the information to direct different or additional training to individuals perceived as more likely to use weak passwords routinely.

The research had several limitations. First, our data were gathered via an online survey in which participants were asked to create a new password. It is possible that the creation of a password in this circumstance would differ from how participants would create a password in their everyday life. In a real-world circumstance in which participants needed to create a new password that they would continue to use indefinitely, they may not only create stronger passwords, but they may pay more attention to messages that they view during the process of creating the password. A second limitation is related to the sampled groups (i.e., university students and MTurk workers), which may differ in important ways from other populations, such as those recruited via social media or using other means. Future research is needed to determine whether our results generalize to different populations. Those involved in developing campaigns to raise awareness about cybersecurity generally and/or the importance of using strong passwords, specifically, might find tailoring campaigns to the population in terms of level of cybersecurity knowledge, education and personality.

In sum, the present study attempted to use a nudge to get people to create stronger passwords. Although the attempt was unsuccessful, we believe that in future research, it may be possible to develop nudges that are effective. The study contributed new knowledge to the literature on predicting who will use stronger passwords. Our results showed that individuals recruited from MTurk created stronger passwords than those recruited from SONA. In addition, on average individuals with higher conscientiousness, higher in emotional stability, higher in knowledge, lower in daily risk taking, and higher in need for cognition created stronger passwords than others.

Declaration of competing interest

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.

Acknowledgement

The research was funded by the National Science Foundation (DGE 1918591 & 1919004).

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.

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.

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, 69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. Retrieved from https://arxiv.org/abs/1901.02672.

Behrend, T. S., Sharek, D. J., Meade, A. W., & Wiebe, E. N. (2011). The viability of crowdsourcing for survey research. *Behavior Research Methods, 43*(3), 800–813. https://doi.org/10.3758/s13428-011-0081-0.

Blais, A. R., & Weber, E. U. (2001). Domain specificity and gender differences in decision making. *Risk, Decision and Policy, 6*, 47–69. https://doi.org/10.1017/S1357530901000254.

Blais, A., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making, 1*(1), 33–47. https://doi.org/10.13072/midss.657.

Bouchard, T. J., & Loehlin, J. C. (2001). Genes, evolution, and personality. *Behavior Genetics, 31*(3), 243–273. https://doi.org/10.1023/A:1012294324713.

Brannon, L. A., & Brock, T. C. (1994). Test of schema correspondence theory of persuasion: Effects of matching an appeal to actual, ideal, and product "selves. In E. M. Clark, T. C. Brock, & D. W. Stewart (Eds.), *Attention, attitude, and affect in response to advertising* (pp. 169–188). Lawrence Erlbaum Associates, Inc.

Brannon, L. A., & Brock, T. C. (2006). Measuring the prototypicality of product categories and exemplars: Implications of schema correspondence theory. *Creating Images and the Psychology of Marketing Communication, 31*.

Brannon, L. A., & McCabe, A. E. (2002). Schema-derived persuasion and perception of AIDS risk. *Health Marketing Quarterly, 20*(2), 31–48. https://doi.org/10.1300/J026v20n02_03.

Brock, T. C., Brannon, L. A., & Bridgwater, C. (1990). Message effectiveness can be increased by matching appeals to recipients' self-schemas: Laboratory demonstrations and a national field experiment. In S. J. Agres, J. A. Edell, & T. M. Dubitsky (Eds.), *Emotion in advertising: Theoretical and practical explorations* (pp. 285–315). Quorum Books.

Bryant, K., & Campbell, J. (2006). User behaviours associated with password security and management. *Australasian Journal of Information Systems, 14*(1). https://doi.org/10.3127/ajis.v14i1.9.

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 editorials: 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.

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing. *Computers in Human Behavior, 29*(6), 2156–2160. https://doi.org/10.1016/j.chb.2013.05.009.

Coakes, S. J. (2005). *SPSS: Analysis without anguish* (12 ed.). John Wiley & Sons.

Conley, J. J. (1985). Longitudinal stability of personality traits: A multi-trait-multimethod-multi-occasion analysis. *Journal of Personality and Social Psychology, 49*(5), 1266–1282. https://doi.org/10.1037/0022-3514.49.5.1266.

Corradini, I. (2020). *Building a Cybersecurity Culture in Organizations*. Springer.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *NDSS, 14*, 23–26.

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013). Does my password go up to eleven? The impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2379–2388). ACM. https://doi.org/10.1145/2470654.2481329.

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.

Faul, F., & Erdfelder, E. (1992). *GPOWER: A priori, post-hoc, and compromise power analyses for MS-DOS [Computer program]*. Bonn, FRG: Bonn University, Department of Psychology.

Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods, 39*, 175–191. https://doi.org/10.3758/BF03193146.

Ferguson, A. J. (2005). Fostering e-mail security awareness: The West Point carronade. *Educause Quarterly, 28*(1), 54–57.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657–666). ACM. https://doi.org/10.1145/1242572.1242661.

Frey, R., Pedroni, A., Mata, R., Rieskamp, J., & Hertwig, R. (2017). Risk preference shares the psychometric structure of major psychological traits. *Science Advances, 3*(10), Article e1701381. https://doi.org/10.1126/sciadv.1701381.

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the second symposium on Useable Privacy and Security* (pp. 44–55). ACM. https://doi.org/10.1145/1143120.1143127.

Golla, M., & Dürmuth, M. (2018). On the accuracy of password strength meters. In *Proceedings of the 2018 ACM SIGSAC* (pp. 1567–1582). ACM. https://doi.org/10.1145/3243734.3243769.

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.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology, 36*(3), 173–192. https://doi.org/10.1080/03601270903183065.

Guo, Y., Zhang, Z., Guo, Y., & Guo, X. (2020). Nudging personalized password policies by understanding users' personality. *Computers & Security*. , Article 101801. https://doi.org/10.1016/j.cose.2020.101801.

Gustafsod, P. E. (1998). Gender Differences in risk perception: Theoretical and methodological perspectives. *Risk Analysis, 18*(6), 805–811. https://doi.org/10.1111/j.1539-6924.1998.tb01123.x.

Halpern, D. (2015). *Inside the Nudge Unit: How small changes can make a big difference*. WH Allen.

Hansen, P. G. (2015). The definition of nudge and libertarian paternalism: Does the hand fit the glove? *European Journal of Risk Regulation, 1*, 1–20. https://doi.org/10.1017/S1867299X00005468.

Hill, B., Foster, J., Elliott, E., Shelton, J., McCain, J., & Gouvier, W. (2013). Need for cognition is related to higher general intelligence, fluid intelligence, and crystallized intelligence, but not working memory. *Journal of Research in Personality, 47*, 22–25. https://doi.org/10.1016/j.jrp.2012.11.001.

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.

Kankane, S., DiRusso, C., & Buckley, C. (2018). Can we nudge users toward better password management? An initial study. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–6). CHI. https://doi.org/10.1145/3170427.3188689.

Keirsey, D., & Bates, M. (1978). *Please understand me: Character and temperament types*. Prometheus Nemesis Co.

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., & Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE symposium on security and privacy* (pp. 523–537). IEEE. https://doi.org/10.1109/SP.2012.38.

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., Wood, E. E., Byrd-Craven, J., & Downing, M. L. (2016). Financial and ethical risk-taking by young adults: A role for family dynamics during childhood. *Cogent Economics & Finance, 4*(1), 1232225. https://doi.org/10.1080/23322039.2016.1232225.

Li, C. (2016). When does web-based personalization really work? The distinction between actual personalization and perceived personalization. *Computers in Human Behavior, 54*, 25–33. https://doi.org/10.1016/j.chb.2015.07.049.

Li, G., Kung, K. T., & Hines, M. (2017). Childhood gender-typed behavior and adolescent sexual orientation: A longitudinal population-based study. *Developmental Psychology, 53*(4), 764. https://doi.org/10.1037/dev0000281.

Linnér, R. K., Biroli, P., Kong, E., Meddens, S. F. W., Wedow, R., Fontana, M. A., Lebreton, M., Tino, S. P., Abdellaoui, A., Hammerschlag, A. R., Nivard, M. G., Okbay, A., Rietveld, C. A., Timshel, P. N., Trzaskowski, M., de Vlaming, R., Zünd, C. L., Bao, Y., Buzdugan, L., Caplin, A. H., et al. (2019). Genome-wide association analyses of risk tolerance and risky behaviors in over 1 million individuals identify hundreds of loci and shared genetic influences. *Nature Genetics, 51*(2), 245–257. https://doi.org/10.1038/s41588-018-0309-3.

Lorenz, B., Kikkas, K., & Klooster, A. (2013). 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* (pp. 276–283). Springer. https://doi.org/10.1007/978-3-642-39345-7_29.

Lowry, D. (1987). Nonverbal communication. In S. Hecker, & D. W. Stewart (Eds.), *Nonverbal communication in advertising*. Lexington Books.

Maraj, A., Martin, M. V., Shane, M., & Mannan, M. (2019). On the null relationship between personality types and passwords. In *7th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada* (pp. 1–7). https://doi.org/10.1109/PST47121.2019.8949024.

McBride, M., Carter, L., & Warkinten, M. (2012). *Exploring the role of individual employee characteristics and personality on employee compliance with cyber security policies. (Prepared by RTI International – Institute for Homeland Security Solutions under contract 3-312-0212782*.

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.

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/10.1080/15332861.2010.487415.

Melicher, W., Ur, B., Segreti, S. M., Komanduri, S., Bauer, L., Christin, N., & Cranor, L. F. (2016). Fast, lean, and accurate: Modeling password guessability using neural networks. In *25th USENIX Security Symposium, 16* pp. 175–191). USENIX Security.

Miller, M. M., & Brannon, L. A. (2015). Influencing college student drinking intentions with social norms and self-schema matched messages: differences between low and high self-monitors. *Health marketing quarterly, 32*(4), 297–312. https://doi.org/10.1080/07359683.2015.1093877.

Narayanan, A., & Shmatikov, V. (2005). November). Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings of the 12th ACM conference on Computer and communications security* (pp. 364–372). ACM. https://doi.org/10.1145/1102120.1102168.

Nikolašević, Ž., Dinić, B. M., Smederevac, S., Sadiković, S., Milovanović, I., Ignjatović, V. B., Prinzd, M., Budimlijae, Z., & Bosić, D. Z. (2021). Common genetic basis of the five factor model facets and intelligence: A twin study. *Personality and Individual Differences, 175*, 110682. https://doi.org/10.1016/j.paid.2021.110682.

Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. In *Proceedings of the Seventh Australasian Conference on Information Security, 98* pp. 71–78).

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.

Panno, A., Donati, M. A., Milioni, M., Chiesi, F., & Primi, C. (2018). Why women take fewer risk than men do: The mediating role of state anxiety. *Sex Roles, 78*(3–4), 286–294. https://doi.org/10.1007/s11199-017-0781-8.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. *Judgment and Decision making, 5*(5), 411–419.

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.

Pease, M. E., Brannon, L. A., & Pilling, V. K. (2006). Increasing selective exposure to health messages by targeting person versus behavior schemas. *Health Communication, 19*(3), 231–240. https://doi.org/10.1207/s15327027hc1903_5.

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior, 109*, 106347. https://doi.org/10.1016/j.chb.2020.106347.

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.

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

Pilling, V. K., & Brannon, L. A. (2007). Assessing college students' attitudes toward responsible drinking messages to identify promising binge drinking intervention strategies. *Health Communication, 22*(3), 265–276. https://doi.org/10.1080/10410230701708121.

Pittman, J., & Robinson, N. (2020, December). Do users correctly identify password strength? *Journal of the Colloquium for Information Systems Security Education, 8*(1), 6-6.

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.

Proctor, W. R. (2016). *Investigating the efficacy of cybersecurity awareness training programs*. Utica College: Unpublished Doctoral dissertation.

Rayner, G., & Lang, T. (2011). Is nudge an effective public health strategy to tackle obesity? No. *BMJ. British Medical Journal, 342*. https://doi.org/10.1136/bmj.d2177.

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2019). May). How well do my results generalize? Comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 1326–1343). IEEE. https://doi.org/10.1109/SP.2019.00014.

Renaud, K., & Zimmermann, V. (2019). Nudging folks towards stronger password choices: Providing certainty is the key. *Behavioural Public Policy, 3*(2), 228–258. https://doi.org/10.1017/bpp.2018.3.

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

Ross, J., Irani, L., Silberman, M. S., Zaldivar, A., & Tomlinson, B. (2010). Who are the crowdworkers: Shifting demographics in mechanical turk. In CHI'10 extended abstracts on Human factors in computing systems. *ACM*, 2863–2872. https://doi.org/10.1145/1753846.1753873.

Russell, J. D., Weems, C. F., Ahmed, I., & Richard, G. G., III (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.

Seitz, T., von Zezschwitz, E., Meitner, S., & Hussmann, H. (2016). Influencing self-selected passwords through suggestions and the decoy effect. In *Proceedings of the 1st European Workshop on Useable Security* (pp. 1–6). Darmstadt: Internet Society. https://doi.org/10.14722/eurousec.2016.2300.

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.

Shou, Y., & Olney, J. (2020). Assessing a domain-specific risk-taking construct: A meta-analysis of reliability of the DOSPERT scale. *Judgment and Decision Making, 15*(1), 112.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. University of Oxford Press.

Tamrakar, A., Russell, J. D., Ahmed, I., Richard, G. G., III, & Weems, C. F. (2016). Spice: A software tool for bridging the gap between end-user's insecure cyber behavior and personality traits. In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy* (pp. 124–126). ACM. https://doi.org/10.1145/2857705.2857744.

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.

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

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.

Thompson, E. R., Prendergast, G. P., & Dericks, G. H. (2021). Do the happy-go-lucky? *Current Psychology*. https://doi.org/10.1007/s12144-019-00554-w (in press).

TrueColors. (2021). About https://truecolorsintl.com/personality-assessment/.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 2988–2997). IEEE. https://doi.org/10.1109/HICSS.2013.196.

Verizon. (2017). Data breach investigations report 2017. Available at https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_ execsummary_en_xg.pdf.

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems, 19*(3).

Weber, E. U., Blais, A.-R., & Betz, E. (2002). A Domain specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making, 15*, 263–290. https://doi.org/10.1002/bdm.414.

Weir, M., Aggarwal, S., De Medeiros, B., & Glodek, B. (2009). Password cracking using probabilistic context-free grammars. In *2009 30th IEEE Symposium on Security and Privacy* (pp. 391–405). IEEE. https://doi.org/10.1109/SP.2009.8.

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.

Yamagata, S., Suzuki, A., Ando, J., Ono, Y., Kijima, N., Yoshimura, K., Ostendorf, F., Angleitner, A., Riemann, R., Spinath, F. M., Livesley, W. J., & Jang, K. L. (2006). Is the genetic structure of human personality universal? A cross-cultural twin study from north America, europe, and asia. *Journal of Personality and Social Psychology, 90*, 987–998. https://doi.org/10.1037/0022-3514.90.6.987.

York, V. K., Brannon, L. A., & Miller, M. M. (2012a). Marketing responsible drinking behavior: Comparing the effectiveness of responsible drinking messages tailored to three possible "personality" conceptualizations. *Health Marketing Quarterly, 29*(1), 49–65. https://doi.org/10.1080/07359683.2012.652578.

York, V. K., Brannon, L. A., & Miller, M. M. (2012b). Increasing the effectiveness of messages promoting responsible undergraduate drinking: Tailoring to personality and matching to context. *Health Communication, 27*(3), 302–309. https://doi.org/10.1080/10410236.2011.585450.

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.