On the null relationship between personality types and passwords

Amit Maraj
Ontario Tech University
Oshawa, Canada
amit.maraj@uoit.ca

Miguel Vargas Martin
Ontario Tech University
Oshawa, Canada
miguel.martin@uoit.ca

Matthew Shane
Ontario Tech University
Oshawa, Canada
matthew.shane@uoit.ca

Mohammad Mannan
Concordia University
Montreal, Canada
m.mannan@concordia.ca

***Abstract*—We performed a preliminary investigation of the relationship between the Big-five personality traits and the strength of selected and created online security passwords. Five-hundred and ten participants were recruited through MTurk and asked a) to complete a Big-five personality inventory, b) to select from a list of available passwords the one they felt was most secure, and c) to create unique, secure passwords for their own online protection. The security strength of participants' selected/created passwords was rated via Zxcvbn, and evaluated on a variety of additional security-based criteria (e.g., password length, inclusion of special characters). In all cases results failed to identify significant relationship between the strength of the selected/chosen password and any Big-five personality traits (when employing appropriately stringent control for multiple corrections). These null results suggest that other factors beyond an individual's personality may hold greater influence over the strength of selected/created online passwords. We present detailed observations and findings from our experiment, discuss potential considerations for contradictions, and suggest possibilities for future research into the password/personality relationship, including the potential use of enhanced password strength meters and tailored security nudges.**

I. Introduction

Considerable research suggests that personality traits may influence the manner in which people interact with online and mobile technologies; see e.g., [1]–[5]. Interesting findings in this domain have for instance demonstrated relationships between specific personality traits and both internet usage [4] and smartphone usage [2]. The Big-five personality traits, in particular, have been shown to predict a wide variety of online behaviors, including internet usage and susceptibility to internet addiction. In one relatively recent demonstration of the predictive validity of the Big-five traits, Cambridge Analytica, a notorious British political consulting firm (now defunct), allegedly used Big-five personality data to guide a targeted ad campaign against unsuspecting Facebook users [6]. The success of this campaign suggests a potential utility for using personality-based information to prey on online users. But could personality profiles also be used to help protect online users? To, perhaps, encourage those who are most vulnerable to online attacks to undertake safer online security practices?

With questions of this nature in mind, the current study sought to evaluate the relationship between personality traits and the security of one's selected/chosen online passwords. Research focused on understanding user's password selection/creation practices is very active; see e.g., password strength [7]–[13], password habits [14]–[17], and effects of strength meters on passwords [18]–[20]), and the majority of work evaluating the strength and guessability of online passwords (e.g., [8], [15], [18], [21]–[23]) have indicated that users tend to choose easy-to-remember passwords that include names, short words, dates, and patterns. However, the extent to which this tendency for weaker passwords reflects the influence of individual personality characteristics remains largely unexplored. Thus, to further research in this understudied area, we conducted an online experiment via Amazon Mechanical Turk (MTurk) within which 510 participants from across the world a) completed a well-validated measure of the Big-five personality traits, and b) selected/created online passwords in a variety of pseudo real-world scenarios. Key to the study was the extent to which individual Big-five characteristics would predict the strength of participants' selected/chosen passwords.

Contributions. Primary contributions included: *i*) a comprehensive analysis of relationships between Big-five personality traits and the strength of 510 MTurk participants selected/created passwords, as evaluated via Zxcvbn; *ii*) a further analysis of potential relationships between Big-five personality traits and specific characteristics of participants' created passwords (i.e., length, use of symbols, digits, etc.); *iii*) a consideration of lessons learned and of potential directions for future work into personality/password relationships.

Summary of Findings. No significant password/personality relationships surpassed stringent control for multiple comparisons, suggesting that factors beyond personality traits may serve as stronger influences of password selection/creation practices. That said, several interesting patterns that met uncorrected significant thresholds may be deserving of future attention: Extroversion correlated positively with the strength of users' passwords, and Openness correlated negatively with password ranking accuracy. Furthermore, exploratory analyses identified additional relationships (uncorrected for multiple comparisons) between Big-five traits and specific characteristics of participants' created passwords. For instance, higher Openness and Extroversion scores predicted shorter passwords that contained fewer letters, while higher Conscientiousness

The first and second authors acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), funding reference number RGPIN-2018-05919.

978-1-7281-3265-5/19/$31.00 ©2019 IEEE

scores predicted passwords that contained fewer symbols. In total, these findings suggest that additional work into password/personality relationships may uncover important relationships; nonetheless, the lack of findings meeting stringent multiple-comparison corrections suggest that more potent predictors of password selection/creation behavior may exist.

II. Related Work

A handful of previous studies have evaluated relationships between personality characteristics and online-/password-related behaviors. Halevi et al. [24] found that participants with higher Neuroticism scores responded more often to phishing emails that touted potential prizes, and that participants with higher Openness scores posted more information on Facebook and had less strict privacy settings. Whitty et al. [25] found that individuals who scored high on self-monitoring were more likely to share their passwords. Additionally, Gratian et al. [26] found that several characteristics including Extroversion (as well as risk-taking, rational decision-making, and gender) related to good security behaviors including: *device securement*, *password generation* and *proactive security awareness* – security behaviors adopted by Egelman and Peer [27] and Egelman et al. [28], who were among the first to correlate these security behaviors to risk-taking preferences and decision-making styles.

A study undertaken by LastPass [29] may be of particular relevance to the present project. This study reported that while 91% of participants recognize the risk of reusing passwords, 61% continue to do so. Moreover, the study found that this reuse of passwords was unaffected by personality characteristics, occurring equally for individuals with two different personality types, referred to as 'Type A' (defined as: controlling, detail-oriented, deliberate, driven), and 'Type B' (defined as: nonchalant, laid back, flexible, preoccupied). This research is intriguing, and provides a valuable first-pass effort into identifying personality characteristics that predispose vulnerability to password attacks. However, the relatively crude separation of Type A/Type B personalities leaves open the possibility that more sophisticated techniques for evaluating personality could provide additional insights. To this end, the present study evaluated participants' personality traits via a well-validated measure of the Big-five personality traits, which is widely used in psychological research, shows consistent and substantive prediction of a wide variety of real-world behaviors, and has more recently shown strong neurobiological underpinnings [30]. To the best of our knowledge, the Big-five personality traits ("Openness", "Neuroticism", "Conscientiousness", "Agreeableness" and "Extroversion") have never been investigated for their influences on passwords.

III. Preliminaries

Zxcvbn [21] was used to evaluate password strength, due to its simplicity and reliability [31]. Participants completed the Mini-IPIP (International Personality Item Pool), a well-validated, 20-item short form (see Appendix) of the Big-five personality traits [32]. The Mini-IPIP scales show acceptable internal consistency, practical utility, and stable test-retest reliability spanning several months [33]. The Big-five personality traits were selected for this study as the model helps discretize personalities on a quantifiable spectrum. Another common scale, the Myers-Briggs [34], with 16 different indicators, provides too many discrete options for the purpose of this research, as the goal is to find similarities between core, overarching dimensions of personalities.

IV. Experiment

A. Design

We used MTurk to recruit participants. Upon clicking the experiment URL hosted on MTurk, participants were forwarded to a web application consisting of several parts: a questionnaire on password behaviors, a password ranking test, various real-world password-related scenarios, and the Mini-IPIP personality test. Each are described in turn below.

1) Preliminary Questionnaire: Every participant was provided an initial questionnaire, consisting of demographic questions, and questions relating to general online-/password-related experiences. Three questions of particular importance (used to segment the data in Section V), were as follows:

1. *"Security Training"*: Have you ever had any security training in the past? (e.g., law enforcement, computer, etc.)
2. *"Password Awareness"*: Have you ever had any password security awareness training? (e.g., learning the characteristics of weaker and stronger passwords)
3. *"Account Hijacking Involvement"*: Have you ever been required to change your password as a result of an account compromise in the past?

2) Password Ranking Test: Participants were presented with five passwords, randomly selected from the pool of passwords prepared for this experiment (with the constraint that one password was randomly selected from each rank given by Zxcvbn). Participants were asked to rank each of these passwords into the following buckets: Very Weak, Weak, Normal, Strong, and Very Strong. Specific instructions to identify differences between strong and weak passwords were not given.

3) Bank/Email Scenarios: Participants were presented with two real-world scenarios relevant to password creation. The first was a bank scenario, which incorporated the following dialogue, adapted from [35]:

"Imagine there was a breach within your **main banking provider's** online banking platform and because of this, your bank has released a notice that says all accounts may have been ***compromised***. Your bank strongly recommends a password change for all accounts. Please **create** a new password below."

The second was an email-based scenario, which incorporated the following dialogue, adpated from [35]:

"Imagine your main **email service provider has been attacked** and that because of the attack, your email service provider is requesting all users change their password. ***This is your main email account and contains very sensitive information.*** Please **create** a password below."

Participants were provided with the following instructions: "**Note 1**: Create the most secure password you feel **comfortable** using and that you'll be able to remember.
Note 2: This password should be different from the one you created in the previous step."

In both scenarios, the target (main banking/email provider), context (compromise), and solution (create a password) were all carefully portrayed. In the Email Scenario, an inclusion of the sensitive nature of the user's email account was provided to ensure all participants took the potential security breach seriously, regardless of the content of participants' actual email accounts. (cf. [15], [36]).

4) Personality Test: Finally, participants completed an online version of the Mini-IPIP, to evaluate the Big-Five personality traits. The following 5-point likert-scale was used for each of the 20 items on this scale: 1) Very Inaccurate; 2) Inaccurate; 3) Neither Inaccurate or Accurate; 4) Accurate; 5) Very Accurate. Scoring of the Big-five personality traits followed standard Mini-IPIP guidelines.

B. Amazon Mechanical Turk

We performed a demographic analysis of our 510 MTurk participants (after the data filtration step discussed in Section V-A). Since the study was in English, participants were recruited only from English-speaking countries including Australia, Canada, UK, and USA. One hundred and fifty participants (55.5% male) were over the age of 40. The majority of participants were distributed normally between the ages of 20 and 40. The distribution of the participants' occupations was as follows: "Business, Executive, Management, and Financial" (15.6%); "Computer Science and IT-Related" (14.5%); "Education, Training, and Library" (11.4%); "Healthcare Support" (6.8%); the remaining being a combination of other professional fields.

TABLE I
SELECTED PASSWORD GUIDELINES. SLOW HASH TIME IS THE SIMULATED TIME IT TAKES THE ZXCVBN ALGORITHM TO CRACK A PASSWORD USING AN OFFLINE ATTACK WITH A SLOW HASHING FUNCTION, SUCH AS BCRYPT, PBKDF2, OR SCRYPT.

Rank	Slow hash time*	Composition
0	$<$ 1 second	8–12 letters
1	1–5 seconds	7–8 letters, 0–1 digit
2	1–60 minutes	7–8 letters, 0–1 digit
3	5 hours – 5 days	4–8 letters, 2–4 digits
4	5 months – 5 years	8–10 letters, 2–5 digits

C. Password Selection

The passwords used within this experiment were drawn from the 2012 LinkedIn password leak, where 6.5 million passwords were exposed [37]. Out of these, a random subset of 22,000 passwords were taken and brute-forced to recover the true plaintext passwords using the tool Uniqpass[1], which includes over six billion entries within a rainbow table. These passwords were then ranked by Zxcvbn (strength between zero and four). To streamline the types of passwords provided to participants, several filtration steps were taken: (a) 50 passwords were randomly selected from every Zxcvbn rank; (b) passwords in languages other than English were discarded (note that many passwords with rank four in Zxcvbn consist mostly of numbers and letters, in seemingly meaningless order; we did not deem those as being in another language so they were included in our study); (c) only passwords that fit the criteria in Table I were used.

Following this filtration, 98 passwords were retained across all Zxcvbn ranks. All of the resulting passwords which ranked 0-3 from Zxcvbn were comprised of English words and numbers, whereas the selected passwords ranked 4 consisted of numbers and letters in seeming meaningless order.

[1]https://github.com/duyetdev/bruteforce-database

V. RESULTS AND ANALYSIS

A. Data Pre-processing

Pre-processing was required to clean and convert the data prior to analysis. We used a few questions for sanity-checking participants' responses. Based on these filtration questions, we discarded responses from seven participants. Thus, we retained responses from 510 participants for full analysis.

Categorical variables such as "Yes", "No", "Somewhat likely", etc., were pre-processed using One-hot encoding. Two metrics were introduced to score how each participant performed on the password ranking activity overall. (a) "Ranked Score Distance" was calculated by summing the distance of error between the correct and incorrect bucket for each password. For example, if participant A placed a password with an estimated Zxcvbn strength of 2 into the "Very Weak" bucket, they would receive a score of two (2 - 0) for miscategorizing the password by two categories. Thus, smaller Distance scores indicated superior ranking performance. (b) "Ranked Score +/-" acted similarly, but awarded one point for every correctly categorized password, and removed a point for every incorrectly categorized password.

For analysis of password characteristics, four features were derived from each of the passwords created in the email and bank scenarios: "Number of characters", "Number of letters", "Number of digits", and "Number of symbols".

B. Data Analysis on Password Strength

Following preprocessing, analysis of the dataset was undertaken using IBM's SPSS [38]. Relationships with Big-five personality traits were investigated through use of correlation and regression analyses, to evaluate both zero-order and shared/unique relationships between personality and password metrics. r refers to the correlation strength, p is the significance, and N is the sample size. Separate analyses were undertaken to evaluate relationships between Big-five personality traits and password metrics in each of the ranked password and created password tasks.

For each, we adopted Bonferroni family-wise error correction procedures to control for multiple comparisons. For instance, in the password creation scenarios, we evaluated

bivariate correlations between each of the 4 password characteristics and each of the 5 personality traits; thus we employed full Bonferroni family-wise error correction to correct for 20 independent comparisons (explored more in Section VI). Note that this provides an extremely conservative test of study hypotheses.

C. Data Analysis on Password Characteristics

We also undertook more exploratory analysis of specific password characteristics, including: "Number of Characters", "Number of Digits", "Number of Letters" and "Number of Symbols". As before, these analyses were conducted separately for the created and selected password scenarios (however, the "Number of Symbols" field was excluded for selected passwords, as we did not provide any passwords with symbols). Analyses utilized both correlation and regression analyses in IBM SPSS, and were conducted across the entire dataset (N=510), and also separately for participants who answered "Yes" (N=154) and "No" (N=356) to the "Account Hijacking" question (based on the expectation that those participants who have encountered an account hijacking incident would have a higher awareness of password and account security). Relationships between the "Account Hijacking", "Password Awareness" and "Security Training" questions are discussed in Section VI.

D. Password Strength Results

TABLE II
PASSWORD STRENGTH RESULTS. CORRELATION RESULTS BETWEEN PERSONALITY DIMENSIONS AND RESPECTIVE EXPERIMENT ACTIVITIES BEFORE BONFERRONI CORRECTION. AH = "ACCOUNT HIJACKING", BC = BANK CREATION SCENARIO, EC = EMAIL CREATION SCENARIO, PR $\rightarrow$ 0 = PASSWORD RANKING ON THE "WEAKEST" PASSWORD BUCKET, PR $\rightarrow$ 4 = PASSWORD RANKING ON THE "STRONGEST" BUCKET. * = SIGNIFICANT WITH $p < 0.05$, ** = SIGNIFICANT WITH $p < 0.01$.

	BC	EC	PR $\rightarrow$ 0	PR $\rightarrow$ 4
AH = "No" (N=154):				
Openness	-0.018	-0.041	0.035	0.030
Neuroticism	-0.081	-0.059	0.027	0.034
Conscientiousness	0.035	0.065	-0.127	-0.043
Agreeableness	-0.029	-0.042	-0.082	0.107
Extroversion	0.151	0.184*	-0.017	0.048
AH = "Yes" (N=356):				
Openness	-0.057	-0.015	-0.136**	-0.050
Neuroticism	0.072	-0.028	-0.056	0.028
Conscientiousness	-0.037	0.018	-0.017	0.029
Agreeableness	0.003	-0.079	-0.007	-0.050
Extroversion	-0.079	-0.099	0.044	0.005
All (N=510):				
Openness	-0.042	-0.023	-0.083	-0.026
Neuroticism	0.030	-0.038	-0.031	0.034
Conscientiousness	-0.021	0.033	-0.049	0.009
Agreeableness	-0.001	-0.069	-0.033	0.002
Extroversion	-0.011	-0.012	0.024	0.019

Initial Bonferonni-corrected analyses elicited no significant effects, suggesting few relationships between participant personality and the strength of their selected/created passwords. That said, it should be noted that Bonferonni-corrections for 20 independent tests provides an extremely conservative test of study hypotheses. To further explore the data, we also cautiously assessed non-corrected findings, to maximize information for future research directions. Even within these non-corrected results, few significant effects were found, however, two noteworthy relationships were identified: Extroversion was positively correlated with the strength of participants' created passwords in the Email Creation Scenario, and Openness was negatively correlated with accuracy of password rankings (r=-0.136, p=0.01).

E. Password Characteristics Results

Both multiple regression and bivariate correlation analyses were conducted to evaluate individual characteristics of participants' created passwords.

For regression analyses, the five Big-five personality characteristics were entered simultaneously into a regression model, to evaluate for potential unique and shared prediction of participants' password characteristics. Thus, four parallel multiple regression analyses were conducted, to evaluate relationships between personality and "Number of Characters" (i.e., length), "Number of Digits", "Number of Letters", and "Number of Symbols". For these analyses, the mean number of characters across both Bank and Email scenarios was used as the predicted variable. Analyses revealed no relationships between the any of the Big-five personality traits and the created password characteristics.

Despite the non-significant regression analyses, we further explored the data via Pearson bivariate correlations. These analyses were conducted across the whole sample, and also separately for participants who answered "Yes" and "No" to the "Account Hijacking" question. Across the whole sample, no bivariate correlations reached significance. However, in participants who answered "No" to the "Account Hijacking" question, Openness, Conscientiousness and Extroversion showed small but significant relationships with specific password characteristics. Specifically, we identified a negative correlation between Openness and both number of characters (r=-0.196, p=0.015), and number of letters used (r=-0.222, p=0.006 respectively). The latter relationship with number of letters remained at a trend level following Bonferroni correction (p=0.006 and α=0.0025).

For full exploration of the dataset, we undertook additional correlational analyses for the Bank Creation and Email Creation scenarios separately. These analyses are truly exploratory, and only intended to provide the reader with the most in-depth consideration of the data. Within the Bank Creation Scenario, one Bonferonni-corrected effect appeared: Conscientiousness correlated negatively with the number of symbols used (r=-0.310, p=0.00009). Additional uncorrected correlations included a negative correlation between Extroversion and both password length (r=-0.180, p=0.025), and number of letters used (r=-0.182, p=0.024). Within the Email Creation Scenario the only relationship was uncorrected: Conscientiousness was negatively correlated with the number of symbols used (r=-0.189, p=0.019).

TABLE III
PASSWORD CHARACTERISTICS RESULTS. CORRELATION RESULTS BETWEEN PERSONALITY DIMENSIONS AND PASSWORD COMPOSITION. AH = "ACCOUNT HIJACKING", PL = PASSWORD LENGTH, #L = NUMBER OF LETTERS, #D = NUMBER OF DIGITS, #S = NUMBER OF SYMBOLS. * = SIGNIFICANT WITH $p < 0.05$, ** = SIGNIFICANT WITH $p < 0.01$.

		PL	#L	#D	#S	PL	#L	#D	#S
AH = "No" (N=154)		Email Creation Scenario				Bank Creation Scenario			
	Openness	-0.081	-0.104	0.087	0.016	-0.196*	-0.222**	0.078	0.022
	Neuroticism	0.012	-0.001	0.009	0.073	0.086	0.062	0.032	0.071
	Conscientiousness	-0.042	-0.013	0.001	-0.189*	-0.052	-0.012	0.039	-0.310**
	Agreeableness	-0.048	-0.038	0.017	-0.090	-0.121	-0.110	0.027	-0.106
	Extroversion	-0.077	-0.056	-0.033	-0.060	-0.180*	-0.182*	0.038	-0.045
AH = "Yes" (N=356)									
	Openness	0.045	0.024	0.046	-0.004	0.037	0.050	-0.018	-0.012
	Neuroticism	-0.115*	-0.105*	-0.023	-0.011	-0.084	-0.057	-0.041	-0.040
	Conscientiousness	0.018	0.021	-0.037	0.067	0.055	0.065	-0.048	0.055
	Agreeableness	0.052	0.011	0.070	0.021	0.041	0.040	0.025	-0.035
	Extroversion	0.046	0.064	-0.046	0.033	0.039	0.064	-0.054	0.009
All (N=510)									
	Openness	-0.003	-0.024	0.054	-0.004	-0.044	-0.047	0.011	-0.008
	Neuroticism	-0.064	-0.064	-0.011	0.020	-0.023	-0.013	-0.020	-0.005
	Conscientiousness	-0.004	0.009	-0.028	-0.007	0.018	0.037	-0.023	-0.040
	Agreeableness	0.008	-0.010	0.052	-0.016	-0.023	-0.021	0.025	-0.057
	Extroversion	-0.005	0.013	-0.043	0.002	-0.042	-0.031	-0.025	-0.009

VI. DISCUSSION AND FUTURE WORK

Different aspects must be taken into consideration when reflecting on the results within this work. We discuss a few of these below.

Questionnaire. The *"Password Awareness"* question in the preliminary questionnaire is somewhat subjective in the sense that participants may answer "No" even if they know the difference between a stronger and weaker password to some extent. The reasoning behind this is the interpretation of "password security awareness training". The subjectivity in this being a formal or informal process raises consideration.

Both email scenarios given to participants within the password selection and creation activities included an excerpt, "***This is your main email account and contains very sensitive information.***" Some participants may not actually use their email as a personal account to store sensitive information, hence these participants may not be able to relate to this scenario as strongly as intended.

Within both the email and bank scenarios, participants were instructed not to use the same password for both instances. The reasoning behind this was to ensure participants were treating both situations as two completely different accounts; but we acknowledge that even mentioning this could have the possibility to skew data in an unauthentic fashion. Although it is understood that we may have primed the participant to some degree and put them on the spot, what we gained from doing this was a more diverse dataset and possibly varying levels of strength within the two created passwords.

Password Selection. Our experiment included a password selection task right before password creation (i.e., a bank password selection before the bank password creation and the email password selection before the email password creation), where participants were greeted with five varying levels of passwords to select from, as ranked by Zxcvbn. We acknowledge that this might have had a priming effect in participants. Nevertheless, such priming would have been consistent across all of the participants, making us believe that it would not have altered the correlations between password characteristics and personality traits. Further studies are needed. Jeske et al. [39] conclude that "nudges can effectively and significantly change behavior" and although this was not confirmed in our experiment, we expected the varying levels of secure passwords in the selection phases would not have influenced the created password in the following creation phases. Though not exactly the same as the password selection activity in this experiment, Ur et al. [18] reported that a combination of visual and text feedback was the most effective intervention in the design of password strength meters. No textual or visual feedback was given to participants after the selection activities. Furthermore, Jeske et al. [39] found that when Wi-Fi networks had the same colored font, while not being ordered by security, no influences on participant selection was observed, implying that security nudges are existent only when done in a certain way. Passwords given to participants in the password selection activities were presented in a similar fashion (i.e., passwords were in a white font inside a gray rectangular box with random ordering).

Password Characteristics. Considering the anticipated analysis on password characteristics, the lack of inclusion of password policies for the password creation activities (bank and email) was of importance. Not having password policies instructing participants to have a minimum number of characters, which included at least one letter, one digit, and one symbol for example allowed participants to freely create a password. Although almost all email providers and online bank sites implement some sort of password policy, the intent behind not having one was to treat the situation as generically as possible, since password policies differ significantly between sites. This also allowed us to perform the password characteristics analysis without much restriction.

Correlations. Although evidence of several uncorrected correlations were obtained, few if any effects withstood correction for multiple comparison. Thus, our findings do not indicate a strong relationship between any of the Big-five personality traits and a variety of password strength metrics. That said, it should be noted that the Bonferroni corrections employed in the present study provided a particularly conservative approach to analysis of study data. Given the existence of several effects at uncorrected levels, including positive relationships with Extroversion, and negative relationships with Openness, we believe additional work into this area may be warranted. This work may choose to make use of a longer, more comprehensive, metric of Big-five characteristics that is capable of evaluating not only the five primary traits, but also the 30 underlying trait facets. Alternately, more ecologically-valid password-relevant scenarios may be employed, to further encourage users to employ more significant safeguarding of their passwords. To ensure an inadvertent cross-correlation was not observed in our tests, a point-biserial correlation analysis was run on the data between "Account Hijacking" and password strength score on all 4 scenarios (email creation, email selection, bank creation and bank selection). It was found that no significant correlations between "Account Hijacking" and password score were present: Bank selection (correlation $r = \quad 0.056$, significance $p = 0.208$), bank creation ($r = \quad 0.068$, $p = 0.126$), email selection ($r = 0.036$, $p = 0.421$), email creation ($r = 0.015$, $p = 0.733$).

Participants. The size of the current study was substantial at 510 participants; moreover, we tested password strength in several diverse ways. Nonetheless, future research could gain additional reliability by making use of a larger sample, or within real-world systems such as, web browsers which can collect a user's personality type, save it, then suggest passwords as required. Furthermore, in our study we determined security expertise based on a user's response about having received security training and the time they spend on the internet. We acknowledge that the use of a framework would have helped us identify with more granularity and accuracy the level of expertise of the participants. To achieve this, future work could make use of an instrumentation like Rajivan et al.'s [40].

Future Work. Although inconclusive due to false discovery rate, our analysis suggested a possible correlation between Extroversion and password strength, particularly when the participant answered "No" to our "Account Hijacking" question. In contrast, Extroversion related somewhat negatively to password strength when participants answered "Yes" to "Account Hijacking." Furthermore, our results seem to suggest that Openness could be positively correlated with the ability to distinguish between stronger and weaker passwords. In addition, when participants answered "No" to "Account Hijacking", password composition analysis seemed to indicate that Extroversion and Openness are directly correlated with creating passwords with fewer letters and more numbers and symbols, and Conscientiousness was directly correlated with creating passwords with fewer symbols. It would also be interesting to investigate more abstract password characteristics and behaviors, and their correlation to individual personality types, e.g., likeliness to use a string of digits or a string of characters, or tendency to share or reuse passwords.

REFERENCES

[1] P. A. Vernon, R. A. Martin, J. A. Schermer, and A. Mackie, "A behavioral genetic investigation of humor styles and their correlations with the Big-5 personality dimensions," *Personality and Individual Differences*, vol. 44, no. 5, pp. 1116–1125, Apr. 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0191886907003984

[2] G. Chittaranjan, J. Blom, and D. Gatica-Perez, "Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones," in *2011 15th Annual International Symposium on Wearable Computers*, Jun. 2011, pp. 29–36.

[3] P. A. Rosen and D. H. Kluemper, "The impact of the Big Five personality traits on the acceptance of social networking website," in *Americas' Conference on Information Systems*, 2008.

[4] N. C. Krämer and S. Winter, "Impression Management 2.0," *Journal of Media Psychology*, vol. 20, no. 3, pp. 106–116, Jan. 2008. [Online]. Available: https://econtent.hogrefe.com/doi/abs/10.1027/1864-1105.20.3.106

[5] T. A. Judge and R. Ilies, "Relationship of personality to performance motivation: A meta-analytic review," *Journal of Applied Psychology*, vol. 87, no. 4, pp. 797–807, 2002.

[6] M. Mirchandani, "To delete or not to #DeleteFacebook, that is the question," *The Wire*, 2018. [Online]. Available: https://thewire.in/media/to-delete-or-not-to-deletefacebook-that-is-the-question

[7] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 162–175. [Online]. Available: http://doi.acm.org/10.1145/1866307.1866327

[8] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 523–537.

[9] S. M. Segreti, W. Melicher, S. Komanduri, D. Melicher, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor, and M. L. Mazurek, "Diversify to survive: Making passwords stronger with adaptive policies," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[10] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Designing password policies for strength and usability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 4, p. 13, 2016.

[11] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay, "Measuring real-world accuracies and biases in modeling password guessability," in *USENIX Security Symposium*, 2015, pp. 463–481.

[12] R. Shay, L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur, "A spoonful of sugar?: The impact of guidance and feedback on password-creation behavior," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2903–2912.

[13] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Can long passwords be secure and usable?" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2927–2936.

[14] D. Florencio and C. Herley, "A large-scale study of Web password habits," in *Proceedings of the 16th International Conference on World Wide Web*, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/1242572.1242661

[15] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proceedings of the Second Symposium on Usable Privacy and Security*, ser. SOUPS '06. New York, NY, USA: ACM, 2006, pp. 44–55. [Online]. Available: http://doi.acm.org/10.1145/1143120.1143127

[16] E. Stobert and R. Biddle, "The password life cycle: user behaviour in managing passwords," in *Proc. SOUPS*, 2014.
[17] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Communications of the ACM*, vol. 58, no. 7, pp. 78–87, 2015.
[18] B. Ur, P. G. Kelley, and S. Komanduri, "How does your password measure up? The effect of strength meters on password creation | USENIX," 2012. [Online]. Available: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur
[19] X. D. C. De Carnavalet, M. Mannan *et al.*, "From very weak to very strong: Analyzing password-strength meters," in *NDSS*, vol. 14, 2014, pp. 23–26.
[20] X. D. C. D. Carnavalet and M. Mannan, "A large-scale evaluation of high-impact password strength meters," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, p. 1, 2015.
[21] D. L. Wheeler, "zxcvbn: Low-budget password strength estimation | USENIX," Aug. 2016. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler
[22] S. Komanduri, R. Shay, L. F. Cranor, C. Herley, and S. E. Schechter, "Telepathwords: Preventing weak passwords by reading users' minds," in *USENIX Security Symposium*, 2014, pp. 591–606.
[23] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, "Fast, lean, and accurate: Modeling password guessability using neural networks," in *USENIX Security Symposium*, 2016, pp. 175–191.
[24] T. Halevi, J. Lewis, and N. Memon, "A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits," in *Proceedings of the 22Nd International Conference on World Wide Web*, ser. WWW '13 Companion. New York, NY, USA: ACM, 2013, pp. 737–744. [Online]. Available: http://doi.acm.org/10.1145/2487788.2488034
[25] M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual differences in cyber security behaviors: An examination of who is sharing passwords," *Cyberpsychology, Behavior and Social Networking*, vol. 18, no. 1, pp. 3–7, Jan. 2015. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4291202/
[26] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security*, vol. 73, pp. 345–358, Mar. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404817302523
[27] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (sebis)," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2873–2882.
[28] S. Egelman, M. Harbach, and E. Peer, "Behavior ever follows intention?: A validation of the security behavior intentions scale (sebis)," in *Proceedings of the 2016 CHI conference on human factors in computing systems*. ACM, 2016, pp. 5257–5261.
[29] V. Lauren, "Introducing the psychology of passwords," *The LastPass Blog*, Sep. 2016. [Online]. Available: https://blog.lastpass.com/2016/09/infographic-introducing-the-psychology-of-passwords.html/
[30] C. G. DeYoung, J. B. Hirsh, M. S. Shane, X. Papademetris, N. Rajeevan, and J. R. Gray, "Testing predictions from personality neuroscience: Brain structure and the big five," *Psychological science*, vol. 21, no. 6, pp. 820–828, 2010.
[31] M. Golla and M. Dürmuth, "On the accuracy of password strength meters," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, 2018.
[32] L. R. Goldberg, "A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models," *Personality Psychology in Europe*, vol. 7, no. 1, pp. 7–28, 1999.
[33] M. B. Donnellan, F. L. Oswald, B. M. Baird, and R. E. Lucas, "The Mini-IPIP Scales: Tiny-yet-effective measures of the Big Five Factors of Personality." *Psychological Assessment*, vol. 18, no. 2, pp. 192–203, 2006.
[34] F. W. Saunders, *Katherine and Isabel: Mother's Light, Daughter's Journey*, first edition ed. Palo Alto, Calif: Nicholas Brealey Publishing, Jan. 1995.
[35] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "Correct horse battery staple: Exploring the usability of system-assigned passphrases," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12. New York, NY, USA: ACM, 2012, pp. 7:1–7:20. [Online]. Available: http://doi.acm.org/10.1145/2335356.2335366
[36] S. Haque, M. Wright, and S. Scielzo, "A study of user password strategy for multiple accounts," in *Proceedings of the third ACM conference on data and application security and privacy*. ACM, 2013, pp. 173–176.
[37] P.-H. Kamp, "LinkedIn Password Leak: Salt Their Hide," *ACM Queue*, vol. 10, no. 6, 2012.
[38] I. SPSS *et al.*, "Ibm spss statistics for windows, version 20.0," *New York: IBM Corp*, 2011.
[39] D. Jeske, L. Coventry, P. Briggs, and A. van Moorsel, "Nudging whom how: IT proficiency, impulse control and secure behaviour," in *Personalizing Behavior Change Technologies CHI Workshop*, 2014.
[40] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "Factors in an end user security expertise instrument," *Information and Computer Security*, vol. 25, no. 2, pp. 190–205, 2017.

APPENDIX

A. The Big-five Personality Indicators

1) **Extroversion** relates to one's degree of outgoingness, particularly in social situations. High levels of Extroversion are characterized by excitability, sociability, talkativeness, assertiveness and high amounts of emotional expressiveness.
2) **Agreeableness** relates to one's level of cooperativeness and concern for others.
3) **Conscientiousness** relates to one's goal-directedness, thoughtfulness, and impulse control.
4) **Neuroticism** relates to one's level of emotional stability. High levels of Neuroticism are characterized by sadness, moodiness, and emotional instability. Those with low Neuroticism tend to be more emotionally stable and emotionally resilient.
5) **Openness** relates to one's ability to see connections between divergent concepts, and willingness to consider other perspectives.

B. Mini-IPIP Personality Test

The following questions were used as a part of the administered personality test for participants.
1. "I am the life of the party",
2. "I sympathize with others' feelings",
3. "I get chores done right away",
4. "I have frequent mood swings",
5. "I have a vivid imagination",
6. "I don't talk a lot",
7. "I am not interested in other people's problems",
8. "I often forget to put things back in their proper place",
9. "I am relaxed most of the time",
10. "I am not interested in abstract ideas",
11. "I talk to a lot of different people at parties",
12. "I feel others' emotions",
13. "I like order",
14. "I get upset easily",
15. "I have difficulty understanding abstract ideas",
16. "I keep in the background",
17. "I am not really interested in others",
18. "I make a mess of things",
19. "I seldom feel blue",
20. "I do not have a good imagination".