6-2021

Impact of Personality Types and Matching Messaging on Password Strength

Anna Bakas
Loyola University Chicago

Anne Wagner
Loyola University Chicago

Spencer Johnston
Loyola University Chicago

Shelia Kennison
Oklahoma State University

Eric Chan-Tin
Loyola University Chicago, dchantin@luc.edu

EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

Impact of Personality Types and Matching Messaging on Password Strength

Anna Bakas[1], Anne Wagner[1], Spencer Johnston[1], Shelia Kennison[2], Eric Chan-Tin[1]

[1]Loyola University Chicago
[2]Oklahoma State University

Abstract

People often create passwords for their accounts that are insecure. An insecure password is often easy to guess – thus, hackers can easily access their victims' accounts. It is important for users to know how to create and manage secure passwords so they can better protect themselves from hackers. It is well-known that different users have different personality types, such as Big Five and True Colors. This research examines if there is any link between personality types and password security behavior. Each participant was shown either a matching or mismatching message based on their personality type, and it was measured whether their password security behavior changed a month later. Our results show that 66% of participants with a Green (knowledgeable and competent) personality type chose a strong password, compared to less than 50% of other personality types. Our results also demonstrate that messaging has a statistical impact on improving password security behavior.

Received on 01 April 2021; accepted on 27 May 2021; published on 01 June 2021

Keywords: Password, Password Strength, Personality, Matching Messages

doi:10.4108/eai.1-6-2021.170012

1. Introduction

In the current age of the Internet, everyone is connected to their devices and accounts. The average person now has 7.6 active social media accounts, and 98% of people have at least one social network account [1]. The average person also has other accounts, such as bank, e-mail, forums, etc. Thus, the number of accounts/passwords that an average person has to be remember is big. All of these platforms, and more, often require the same thing: a password. Passwords ensure the security of an online account. Most passwords are generated by users [2], [3], [4]. Insecure passwords are not the only problem to plague users, but also password reuse [5]. If passwords are reused over multiple accounts such as social media and banking, then not only is a user's social presence compromised but also their financial information. When password insecurity and reuse are combined, it makes it even easier for hackers to steal information from different platforms on the Internet. Thus, it is vital for users to know how to create and manage strong, secure passwords. A strong password consists of letters, numbers, and special symbols, and has enough characters to prevent brute-forcing. Creating strong passwords and having different ones for each account keep users protected. However, strong passwords are hard to remember, which makes using password managers very helpful.

It has been extensively studied that different people have different personality traits. The Big Five personality traits [6] are openness, conscientiousness, extraversion, agreeableness, and neuroticism. The four True Colors [7] personality types are orange, gold, green, and blue. Orange personalities tend to be energetic, charming, and spontaneous. Gold personalities tend to be punctual, organized, and precise. Green personalities tend to be analytical, intuitive, and visionary. Blue personalities tend to be compassionate, cooperative, and emphatic.

A survey was created to measure participants' personality traits, demographics information, and password usage and knowledge. Each participant also completed the Human Aspects of Information Security Questionnaire (HAIS-Q) [8], which measures knowledge about information security. Each participant is also presented with either a matching or mismatching

*Anna Bakas. Email: abakas@luc.edu

message, depending on the participant's True Colors personality or self schemas [9]. For example, a blue personality might be matched with a blue message about caring for others and making sure their accounts do not get hacked due to weak passwords. Finally, each participant is asked to type in a password they consider to be strong.

The goal of this research is to determine if there is any link between the Big Five or True Colors self schemas and password usage and management. The matching messages will be evaluated whether they work in changing password security behavior. This builds upon previous work [10–15] which have shown that matching messages based on personality types have changed health-related behaviors such as AIDS and drinking. The motivation for this research is that if a certain personality type(s) or self schema(s) tends to exhibit insecure behaviors, more targeted cybersecurity training/education can be performed on these people. Moreover, a generic "pick a strong" password message might not resonate well with everybody, thus designing matching messsaging is hypothesized to have a higher impact.

The research questions and contributions of this research are

- is there any relationship between personality and password strength, that is, does a certain personality tend to pick stronger passwords than others?
- is there any link between information security knowledge and password security behavior?
- does a matching message based on personality type improve security knowledge and behavior?

Although we could find no relationship between the Big Five personality traits and password strength, we found that the Green True Colors self schemas tended to pick strong passwords. Moreover, participants who knew more about password security tended to pick stronger passwords. Finally, messaging about password security improves the information security knowledge of the participants (statistically significant).

The paper is organized as follows. In Section 2, we describe password strengths, personality traits, our matching messages, and give an overview of related work. Section 3 shows the setup of the experiments while Section 4 shows the results of the experiments. Discussion and limitations of the work are described in Section 5. We conclude in Section 6.

2. Background

We provide an overview on the importance of passwords, how to measure password strength, personality traits and types, and matching messages.

2.1. Passwords

To ensure the security of data and personal information, users are often asked to create strong passwords. Passwords are used to prevent unauthorized access to computers, smartphones, and online accounts. However, it is well known that users pick weak passwords and reuse the same passwords for different accounts [5, 16]. The security of an online account is often measured by the strength of the password used. There are different ways to measure the strength of a password [17]. When users are asked to create strong passwords, the requirements that they are asked to satisfy can sometimes be overwhelming: uppercase letters, lowercase letters, symbols, numbers, and longer than eight characters. Long, complex passwords provide security, but on the other hand, they present an inconvenience to users [18–20]. They are difficult to remember and require precision when entering (especially on a smartphone). Password managers [21–23] can help to alleviate this complexity by storing passwords for users to reference later. Multi-factor authentication allows for using multiple factors, such as a password and proof that the user owns a certain phone number, to login.

zxcvbn [24] is a password strength estimator, developed by Dropbox, where passwords are scored on a range from zero to four. Passwords are scored through a combination of pattern matching, recognizing and weighing 30,000 common passwords, common names, popular English words, and other common patterns such as dates, repeats, sequences, and keyboard patterns. A password score/strength of zero means that the password is "too guessable" while a password score of four means that the password is "very unguessable". This tool was picked because it is open source and used by Dropbox, Dashlane, and other well-known companies.

2.2. Personality Traits

It has been shown that individual differences in personality can be described as differences in traits (e.g., extraversion, conscientiousness, agreeableness, etc.). There are many models to measure personality traits – one of the most popular is the Big Five personality traits [6, 25], which are related to the Myers-Biggs personality types [26, 27], and the True Colors self schemas [7].

Big Five. The Big Five personality traits is a model of personality types that has five broad personality types [6, 25].

- Openness. People who enjoy learning and experiencing new things. Traits include being insightful, imaginative, and having a wide variety of interests.

- Conscientiousness. People who are reliable and prompt. Traits include being organized, methodical, and thorough.
- Extraversion. People that enjoy interacting with others. Traits include being energetic, talkative, and assertive.
- Agreeableness. People that are friendly, cooperative, and compassionate. Traits include being kind, affectionate, and sympathetic.
- Neuroticism. People that experience emotional instability and negative emotions. Traits include being moody and tense.

True Colors. True Colors is a personality profiling system that uses four colors for categorizing personality types or self schemas [7].

- Blue. People that are empathetic, compassionate, and cooperative.
- Orange. People that are energetic, spontaneous, and charming.
- Gold. People that are punctual, organized, and precise.
- Green. People that are analytical, intuitive, and visionary.

2.3. Matching Messages

Generic messaging has been used, such as to teach about phishing, using strong passwords, and other cybersecurity behaviors [28–30]. As mentioned earlier, every person has a certain personality type/trait. The purpose of targeted messaging, based on a user's self schema, is to change the user's behavior by showing that user a matching message based on their personality. As an example, introverted users might see a message such as "If your account gets hacked, you will have to communicate with a lot of people to repair the damage done to your accounts, forcing you to deal with new and unfamiliar situations". This message hearkens back to introverts' characteristics of wanting to keep to themselves and live a quieter lifestyle. An introvert would not want to be put in unfamiliar situations, so the message may influence them to take the time to create a strong password as to avoid those situations that could make them uncomfortable.

A mismatching message is a message that is not related to the user's personality. An example is showing a message about neuroticism to an introvert. The hypothesis is that a user shown a matching message about using stronger passwords will be more likely to change their behavior regarding passwords than a user shown a mismatching message.

2.4. Related Work

Generic messaging have been shown [31, 32] that they are not effective. Users either do not follow the advice or revert to insecure behaviors after a certain amount of time. Targeted messaging has been shown to be successful. Requests that are written in a specific way are shown to increase the chance that a person will comply [33–35]. Matching messaging, based on personality types, has also been shown to work in health-related behaviors such as for AIDS risk and drinking risks and behaviors; these matching messages are consistent over time as well [10–15]. This work explores whether matching messages can change password security behavior. We display either a matching or mismatching message to each participant in our study, based on their True Colors self schema. The second part of the study determines whether the matching messaging changed the participants' behavior regarding password security.

Whenever security is involved, it has long been argued that users should be included and are not to blame [36]. Although, [37] shows that there is no relationship between personality types and passwords, we found that the green True Color self schema tends to choose stronger passwords than other self schemas. Previous work [38] has found that neuroticism leads to a higher chance of falling victim to phishing e-mails and that openness leads to posting more information on social media. The effect of cognitive depletion on password creation is shown in [39] – our work assumes no cognitive depletion but considers the effect of matching messages instead. Extraversion is shown in [40] to be related to better security behaviors. Our work focuses on the True Colors self schemas to target the matching messages, instead of the Big Five personality traits. We show that there is a relationship between the self schema and password security and that password behavior can be changed based on the self schema.

3. Experimental Setup

3.1. Survey

We created an online survey, consisting of two parts. The survey asks general questions about the participant's personality, experiences on the Internet, password usage, password behavior, social media usage, and demographics information. Each question of the survey could be skipped. One month after the first part of the survey, each participant was asked to fill out the second part. When printed out, part 1 is 52 pages long and part 2 is 20 pages long; the full survey is thus omitted even from the appendix. Only the most relevant part of the survey are included.

More specifically, part 1 of the survey includes the following questions and information.

- information page about what the survey will contain, that it is a 2-part survey, and that it is expected to take less than 60 minutes.
- each participant is asked to create a unique code that they will have to remember for part 2 so that their responses can be linked. The code is 7 characters long. Each participant was asked to create the code as follows: the first letter of the first name, the day of birth, the month of birth, the first letter of the middle name (X if no middle name), and the first letter of the city they were born in.
- questions about technology usage, such as how many devices/applications that require a password, do they use smartphones, do they use passwords and the type of password used, and whether they know about password managers.
- three questions about what participants think make up a "strong" password.
- the Human Aspects of Information Security Questionnaire (HAIS-Q) [8] questionnaire to measure the participants' information security knowledge.
- several password choices are shown such as *password*, *Password123*, *F63$uj2*, and *doghenry*. Participants are asked whether they think these passwords are strong and whether they are likely to use these passwords.
- questions regarding password security knowledge, such as *I know a lot about password security practices*.
- behavioral questions such as *I would prefer complex to simple problems*.
- personality traits for the Big Five, such as *bold*, *bashful*, etc.
- self schemas for True Colors.
- risky behavioral questions such as *betting a day's income at the horse races*.
- social media usage.
- an "attention" question that asked participants to pick the fourth option.
- matching/mismatching messages, which are described next.
- participants are asked to enter a password that they consider to be strong. The password has to be at least 8 characters. All participants were anonymized using a unique code, but the actual password had to be stored so that it can be evaluated.
- demographics information.

Based on each participant's True Colors self schema, either a matching or mismatching message is shown. For example, if the True Colors self schema is orange, a matching message would be an orange message. A mismatching message would be either a green, gold, or blue message. The messages were created/inspired based on previous works' messages [10–15]. Each matching message is shown next.

Orange Everyone knows you are a person who is adventurous, spontaneous, and fun. If your accounts are hacked, this can create a hassle in your life that can negatively affect your ability to interact with your friends online. As you know, all of your online accounts – including social media, email, and banking – require passwords each time you log in. A strong password is the best protection from hackers. The strongest passwords contain uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, &, @, *, etc.). Also, the strongest passwords are used for only one account, so different accounts should have different passwords. When you get hacked, the hacker wins and you lose. The best way to beat the hacker is to use the strongest passwords, so that you will have time to enjoy your life without being bothered by the inconvenience of dealing with a hacked account. Act now and make sure all your accounts are secure by creating strong passwords.

Gold Everyone knows you are a person who is responsible, organized, and cooperative. If your accounts are hacked, this can lead to chaos in your life. As you know, all of your online accounts – including social media, email, and banking – require passwords each time you log in. A strong password is the best protection from hackers. The strongest passwords contain uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, &, @, *, etc.). Also, the strongest passwords are used for only one account, so different accounts should have different passwords. The disruption from getting hacked could greatly impact all that you have planned for your future and take time to recover from. Having your account stolen by a hacker also means that others in your life might think you are no longer dependable or responsible. Take the time and add the following to your plan as soon as possible: create a strong password for each online account!

Green Everyone knows you are a person who is knowledgeable, competent, and curious. If your accounts are hacked, this can lead to a feeling of incompetence or unintelligence. As you know, all of

your online accounts – including social media, email, and banking – require passwords each time you log in. A strong password is the best protection from hackers. The strongest passwords contain uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, &, @, *, etc.). Also, the strongest passwords are used for only one account, so different accounts should have different passwords. A weak password can easily be guessed by hackers. The rational thing to do is to review all your passwords and strengthen the ones that are weak. Furthermore, weak passwords might make you seem incompetent or irrational. Figuring out how to make your passwords stronger is like solving a complex problem and you are the kind of person who is great at solving problems. Be innovative and competent by creating a strong password. You'll never go wrong when you have the strongest passwords.

Blue Everyone knows you are a person who is compassionate, empathetic, and kind. If your accounts are hacked, this can damage your relationships and disrupt the harmony in your life. As you know, all of your online accounts, including social media, email, and banking, require passwords each time you log in. A strong password is the best protection from hackers. The strongest passwords contain uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, &, @, *, etc.). Also, the strongest passwords are used for only one account, so different accounts should have different passwords. If your accounts get hacked, this means that someone else could pretend to be you to your family, friends and the general public. If the hacker gains control of your accounts, they may say things that make other people think you are being uncaring or insensitive. You are the kind of person who definitely wants to show you are considerate of others. Take a few extra seconds to be considerate of the people in your life by creating strong passwords.

The messages were constructed using the latest password security recommendations on how to create a strong password. The messages were pilot using a small group to ensure that the message is related to the personality self-schema.

Part 2 of the survey includes the following questions. Most of the questions are similar to Part 1.

- similar information page as part 1. Part 2 is expected to take 20 minutes to complete.
- the unique code entered in part 1.
- the strong password entered in part 1, if the participants remembered it.
- open-ended self-reflection about whether the participants had thought about password security and password security practices.
- the HAIS-Q questions.
- password knowledge questions.
- technology usage.
- what constitutes a strong password.
- an attention question.
- several password choices are shown. Participants are asked whether they think these passwords are strong and whether they are likely to use these passwords.
- questions regarding password security knowledge.
- social media usage.
- demographics information.

3.2. Data Collection

The survey is deployed online using Qualtrics. Participants were recruited from a major university's pool of students taking the required first psychology course. These students can be any major at the university and are generally in the 18 to 21 years of age range. Each participant was compensated with 1 credit for the course for completing part 1 of the survey and an additional 0.5 credit for completing part 2 of the survey.

The survey and recruitment process were approved by our IRB office. Data collection took place from September to December 2019.

3.3. Summary of Data

254 people participated in the survey. 28% of participants were men, and 72% were women. 66% of participants were first year, 19% were sophomores, 9% were juniors, and 6% were seniors.

Using zxcvbn [24], a password strength estimator, passwords are scored on a range from zero to four. Passwords are scored through a combination of pattern matching, recognizing and weighing 30,000 common passwords, common names, popular English words, and other common patterns such as dates, repeats, sequences, and keyboard patterns. A password strength score of zero means the password is "too guessable" and a password score of four means the password is "very unguessable". The results of this research will determine how personality types are connected to the strength of the passwords users create.

Analysis of the passwords entered in part 1 of the survey is shown in Figure 1. It can be seen that 105 participants' passwords received a score of one, 54 participants have a score of two, 35 participants a score of three, and 60 passwords received a score of four. This shows that most participants picked a "weak" password.

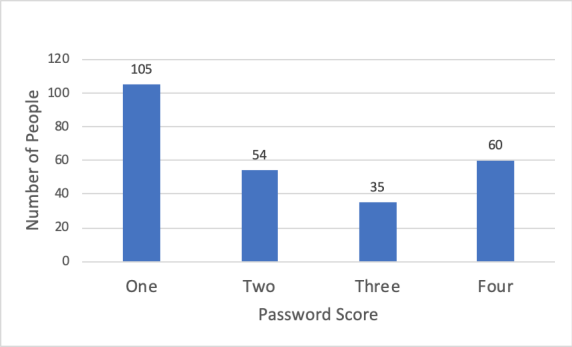

Figure 1. Breakdown of participants' zxcvbn password strength scores.

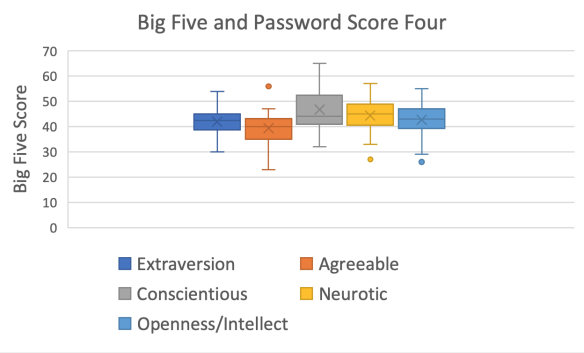

Figure 2. Big Five personality traits and password strength. This graph only includes zxcvbn password score four.

4. Results

The results of our survey are shown. The research questions to be answered are 1) Are certain personality types (either Big Five or True Colors) more likely to pick stronger passwords? 2) Are participants, who know more about password security, more likely to select a stronger password? 3) Is there a link between the HAIS-Q result and password strength? 4) Do matching messages improve cybersecurity behavior, especially related to password security?

4.1. Big Five and Password Strengths

First, we look at whether participants with some Big Five personality traits pick stronger passwords. A person usually has one dominant personality trait (sometimes more than one) and the other personality traits are not as strong in affecting that person's behavior.

To obtain the Big Five personality trait for each participant, we use the mini-marker big five score-sheet [41]. Based on the responses from the survey, each participant had each of the five personality traits scored. The calculation, as described in [41], created a "score" from 8 to 72 for each personality trait.

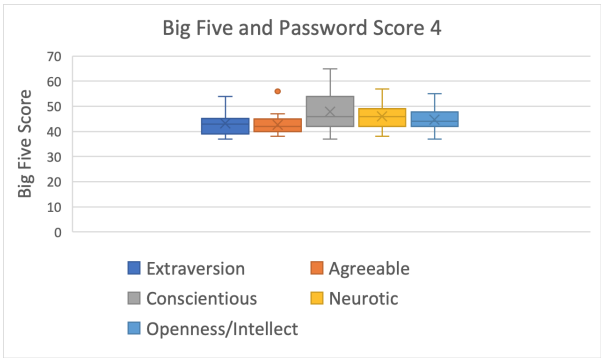

Figure 3. Big Five personality traits and password strength. This graph only includes zxcvbn password score four and Big Five personality trait scores above 36.

Figure 2 shows the relationship between participants who received a password score of four from zxcvbn and their corresponding Big Five personality traits. All of the Big Five personality types are represented in the figure: extraversion, agreeableness, conscientiousness, neuroticism, and openness/intellect (in that order). Figure 2 shows that participants who created a strong password with strength four tend to have higher conscientiousness trait and lower agreeableness trait. This demonstrates that people who are highly conscientious tend to pick stronger passwords than those whose dominant Big Five personality type is agreeableness.

Figure 3 shows the relationship between participants who received a password score of four from zxcvbn and their corresponding Big Five personality traits. To look at participants with the strongest of each Big Five personality type, only participants with Big Five personality scores of above 36 were included. 36 is 50% of 72 which is the highest score. A score greater than 50% indicate that the participant has some of that personality trait. Similar to Figure 2, Figure 3 shows that participants who are highly conscientious tend to pick a stronger password than those who are agreeable or extraverted.

Figure 4 shows the percentage of participants with each Big Five personality type for each zxcvbn password score. This graph conveys that there is not much of a relationship between Big Five personality types and password strength. For each password strength score, there is roughly the same amount of participants who picked a password with that score regardless of their personality traits. This is in line with previous work [37].

4.2. True Colors and Password Strengths

Even though a person usually has one dominant personality trait, that person can also have other strong personality traits. As an example, a person can score

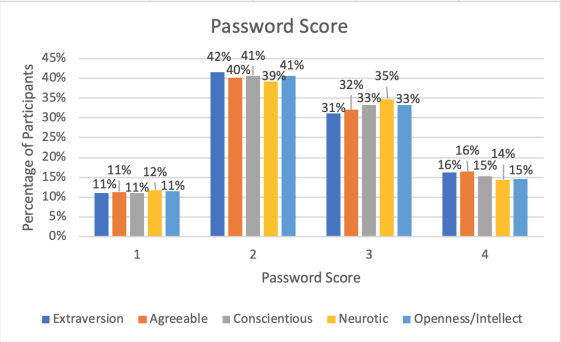

Figure 4. Big Five personality traits and password scores. This graph only includes Big Five personality trait scores above 36.

highly on two personality traits (for example, a score of 71 for agreeableness and a score of 70 for extraversion). There were 79 participants with a tie between two personality traits, 13 participants with two ties between two different personality traits, 12 participants with a three-way tie between three personality traits, and 1 person with a four-way tie between four personality traits. For this reason, we turn to examining the True Colors self schemas. A person usually tends to fall into only one self schema, thus the matching message can be more easily targeted. For True Colors, 105 participants were blue, 54 were gold, 35 were green, and 60 were orange.

To determine a participant's True Colors self schema, the survey included four images as shown in Figure 5. Each participant was asked to select the image and the description that most closely resemble them. The full description of the text in each image is given next.

- 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.

Figure 5. The four images to determine a participant's True Colors self schema. Image A says "I am warm, communicative, compassionate, and feeling". Image B says "I need to be responsible, dependable, helpful, and sensible". Image C says "I am versatile, wise, conceptual, and curious". Image D says "I am adventurous, skillful, competitive, and spontaneous". The full description is given within the text of the paper.

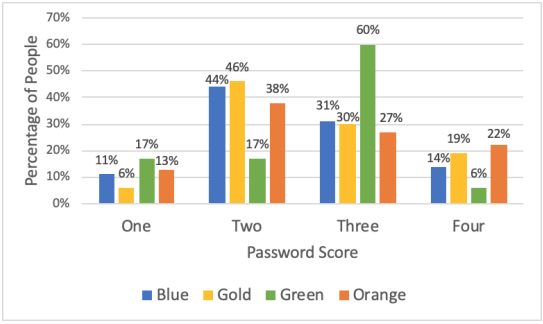

Figure 6. True Colors self schema and password strength according to zxcvbn.

Figure 6 shows the relationship between participants' True Colors self schemas and their password strength

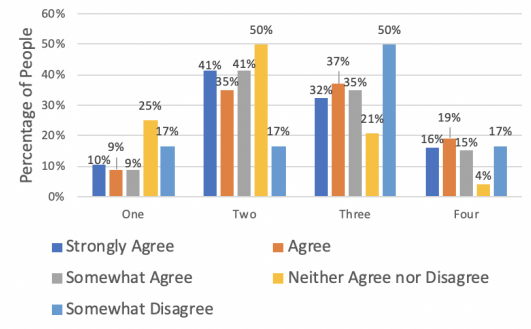

Figure 7. Responses to question about the use of strong passwords and password scores.

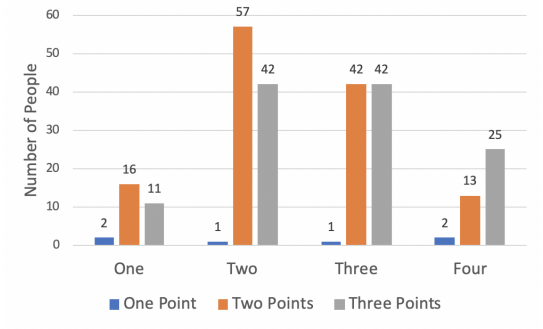

Figure 8. Responses about the characteristics of strong passwords. The x-axis is the password score from zxcvbn while each bar chart is the points value based on the participants' response to three questions.

scores, breaking down how many participants for each self schema picked a particular password score. No participant wrote a password that was given a password score of zero. All of the True Colors self schemas are represented in the figure: blue, gold, green, and orange (in that order). Figure 6 shows that there is a higher percentage of people with a green personality to select a password with password strength score of three. 66% of participants with a green self schema picked a password with scores of three and four, compared to 46% for blue self schema, 49% for gold self schema, and 49% for orange self schema. Green self schemas tend to be knowledgeable and competent. Although that might seem intuitive that green self schemas tend to pick stronger passwords, gold self schemas tend to be organized, which could be interpreted as more organized or knowledgeable in security practices.

4.3. Security Behavior & Password Strengths

As part of the survey, we asked the participants questions about their views on password security and what they think constitutes a strong password. It is expected that participants who think strong passwords are important to secure their online accounts or know that longer passwords are more secure than shorter passwords, would be more likely to create a strong password, as measured by zxcvbn.

Responses about the use of strong passwords in relation to password scores. Figure 7 shows participants' responses to being asked whether strong passwords ensure that accounts are safe and harder to hack into, even if they are inconvenient to use. Participants could answer with strongly agree, agree, somewhat agree, neither agree nor disagree, disagree, somewhat disagree, or strongly disagree. Disagree and strongly disagree answers each only had one participant response; so, that data has been omitted. Figure 7 shows that participants who strongly agreed or agreed with this statement had stronger passwords than those who somewhat disagreed. Combining strongly agree and agree responses, 35% of participants received a password score of four versus 17% of participants who received a password score of four but responded with "somewhat disagree." 4% of participants who responded with "neither agree nor disagree" received a password score of four.

Responses about the characteristics of strong passwords in relation to password scores. Figure 8 shows the relationship between participants' password scores and their responses to what they considered a strong password should have. Participants were asked a series of questions with multiple answer choices, as shown below.

- When you try to think of a password you consider "strong", that is, hard for someone to guess, how many characters does it usually have?
  - 4 characters
  - 5 characters
  - 6 characters
  - 7 characters
  - 8 characters
  - More than 8 characters
- When you try to think of a password you consider "strong", that is, hard for someone to guess, does the password include uppercase letters?
  - Yes
  - No
- When you try to think of a password you consider "strong", that is, hard for someone to guess, does the password include numbers?
  - Yes
  - No

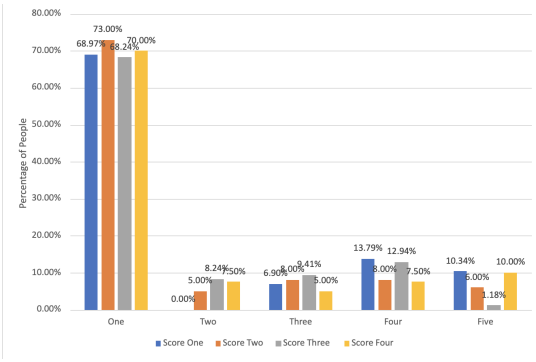

Figure 9. Likelihood of using the password "Password123" and password strength score. In this figure, the bar charts indicate the password score as measured by zxcvbn. The x-axis indicates how likely a participant says they are to use this password – 1 is "not likely" and 5 is "likely".

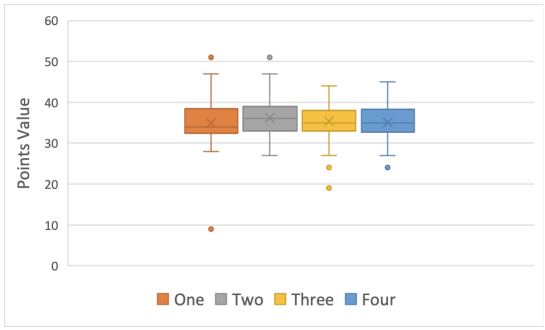

Figure 10. HAIS-Q score and password strength.

Participants' answers were assigned a score (this is a separate score from zxcvbn password strength score) by assigning each answer for the three questions a point value and then totaling the points. For the first question, "4 characters", "5 characters", "6 characters", "7 characters", and "8 characters" each had a point value of zero. "More than 8 characters" had a point value of one. For the second question about uppercase letters, answering "yes" warranted one point while answering "no" warranted zero point. For the third question about numbers, answering "yes" warranted one point while answering "no" warranted zero points. Zero was the minimum score and three was the maximum score participants could receive. No participant received a score of zero. Figure 8 shows how many participants scored what point value based on their password score. The x-axis in the figure is the password score from zxcvbn. Each of the bar chart represents each of the possible points value (recall no participant received a zero score). Figure 8 shows that a higher number of participants who had a password score of four obtained a points value of three, the maximum total score for the questions. 25 participants with a password score of four scored a three. This demonstrates that participants who recognize the characteristics of a strong password (more than 8 characters, include uppercase letters, include numbers) tend to create stronger passwords themselves. Participants with a points value of one were as likely to create a strong password (with password score of four) and a weak password (with password score of one).

Responses about using certain passwords in relation to password scores. Figure 9 shows the relationship between participants' password scores and their response to how likely they were to use the password "Password123" themselves. Participants could answer on a scale from one to five, with one being "not likely" and five being "likely". Figure 9 shows that participants who received a lower password score were more likely to use "Password123" as a password versus those who received a higher password score of three or four – 16% vs 11%. The difference is not high and this indicates that better password education and better matching messaging are needed.

4.4. HAIS-Q/Security Knowledge and Password Strengths

Our survey measured participants' security knowledge. This is performed through two methods. The first method is using the Human Aspects of Information Security Questionnaire (HAIS-Q) [8]. This is a mini survey about information security knowledge, consisting of nine questions. It includes questions such as "It's acceptable to use my social media passwords on my work accounts" and "It's a bad idea to share my work passwords, even if a colleague asks for it". Participants were asked to select the choice that best described them for each question. The answer choices included strongly disagree, disagree, somewhat disagree, neither agree nor disagree, somewhat agree, agree, and strongly agree. Each answer choice was assigned a point value. Strongly disagree had a point value of one, disagree had a point value of two, and so on until strongly agree with a point value of seven. We calculated the total points for each participant. The higher the number of points, the more knowledgeable about security the participant is. For some questions (e.g. "It's acceptable to use my social media passwords on my work accounts"), the point is reversed, meaning that if the participant "strongly agree", instead of 7 points, the participant is assigned 1 point. The maximum points value is 63 and the minimum points value is 9.

Figure 10 shows the relationship between participants' password strength score and their HAIS-Q points total after being presented with the nine statements/questions. The maximum point total that a participant received was 51, and the minimum point total that a participant received was nine, which is the lowest

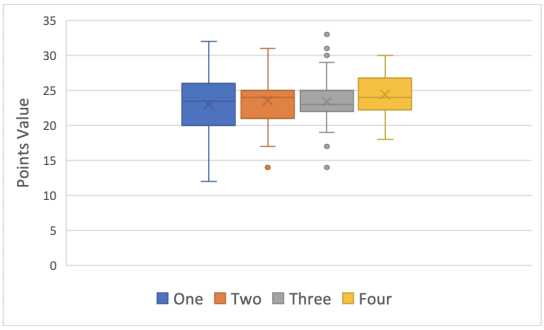

Figure 11. Password security knowledge and password strength.

possible points value. Figure 10 shows the box-and-whisker plot. The "X" indicates the average value and the middle bar is the median value. The bars indicate the first and third quartiles while the whiskers indicate the lowest and highest data points excluding outliers. The dots represent the outliers. The median points total for password score four was 35.15 versus 34.93 for password score one. This is not statistically significant; the figure shows that regardless of HAIS-Q points value, a participant is as likely to create a strong password as a weak password. This would seem to indicate that HAIS-Q is not a good predictor of choosing a strong password but more work is needed to confirm this result.

The second method to measure participants' security knowledge is to ask six questions of our own. The six questions are as follows.

- When creating a password, I always try to create one that is rated as "strong."
- Having "strong" passwords is a top priority for me.
- Usually, I do not make an effort to create passwords that are rated as "strong."
- If my password is rated as "weak," that is usually okay with me.
- I am concerned about the security of my passwords.
- I think that the danger from having weak passwords is exaggerated.

Each participant was asked how much they agreed/disagreed with each statement on a 7-point Likert scale similar to the HAIS-Q scale. Similarly to calculating the HAIS-Q points value, we calculated the points value by adding up the points for each question and reversing the points as needed. The maximum possible points value was 42 and the minimum possible points value is 6.

Figure 11 shows the relationship between participants' password strength score and their points total after being asked how much they agreed or disagreed with the six statements about password security. The maximum point total that a participant received was 33, and the minimum point total that a participant received was 12. Compared to Figure 10, Figure 11 shows that participants who had a score of four had higher points value than those whose password received a password score of one. Password score four's points total was also more compact than password score one's. This demonstrates that those participants were more likely to often pick strongly agree or agree to statements such as, "I am concerned about the security of my passwords" or "Having strong passwords is a top priority for me". The median point total for password score four was 24.2 versus 23 for password score one which conveys how, on average, people who agree with strong password practices tend to create stronger passwords. The average point total for password score four was 24.4 versus 23 for password score one. This could be a significant result, especially since HAIS-Q which is a popular survey on information security, did not yield any correlation with password strength. This means that the HAIS-Q survey could be complemented with our six questions. This could also mean that information security is a broad area and generalized questions do not capture every password of security. A more personalized approach to each area of security might yield more useful results.

4.5. Matching Messages

One month after each participant completed part 1 of the survey, they were asked to complete part 2. Part 2 was estimated to take 20 minutes to complete and each participant was credited with 0.5 credit for completing part 2 of the survey. In part 1 of the survey, there were 254 participants. In part 2 of the survey, we received 153 responses. This is normal for any multi-part survey to have a reduced participation rate in later parts. The responses for each part can be linked due to the unique code entered by the participants. We note that some participants likely forgot their self-created code as there was no matching code for part 1. For some of the codes, we were able to match if it was a simple mistake – for example, a few participants flipped the numbers (07 to 70 possibly due to a transposition error). In the end, we ended up with 132 participants for part 2.

We now determine if matching messages had an effect on password security behavior. Recall that every participant had a True Colors self schema. In the survey, each participant was randomly assigned to either receive a matching message based on their True Colors or one of the three mismatching messages. The expectation is that participants receiving a matching message will get nudged to better security behavior and higher security knowledge. Out of the 132 participants

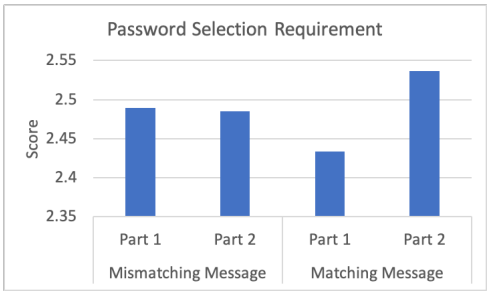

Figure 12. Password Selection Requirement Scores

in part 2 of the survey, 70 received a mismatching message and 62 received a matching message.

General Password Attitudes. Recall from Section 4.3 where participants were asked what they think a "strong" password is made up of. Participants were shown 3 statements about the elements of a strong password, and were assigned 1 point if they agreed with the statements and 0 if they disagreed. The maximum point total that a participant received was 3, while the minimum was 0. Figure 12 shows the responses for part 1 of the survey and part 2 of the survey. The figure also shows whether the participants were shown a matching or a mismatching message. Figure 12 shows that participants with a mismatching message scored the same after part 2 (2.48 in part 2 and 2.49 in part 1), but those participants shown a matching message had a higher points value (2.54 in part 2 vs 2.43 in part 1). This shows that participants change their behavior after being shown a matching message.

HAIS-Q: We next analyze if participants' information security knowledge improved after part 1 of the survey. We looked at the HAIS-Q score. For ease of calculation, we calculated the average score rather than the total score. The average score can range from 1 to 7. For those participants shown a mismatching message, their average score increased from 5.32 in part 1 to 5.78 in part 2. For those participants shown a matching message, their average score increased from 5.31 in part 1 to 5.78 in part 2. When running the ANOVA test, the p-value was 0.002 which indicates that all participants, regardless of message, increased their information security knowledge. However, it is not clear that matching messages had a better effect than mismatching messages (p-value > 0.005). An ANOVA test is a method to determine if a result is significant.

When drilling further into the True Colors self schema, a similar result is obtained. There is no statistical evidence that matching messages had a higher effect than mismatching messages. However, overall the HAIS-Q score increased for all True Colors self schemas (p-value is 0.47). Table 1 shows the average HAIS-Q score for each self schema for both part 1 and part 2. It can be seen that the score increased for all

True Colors Self Schema	HAIS-Q Average Score for Part 1	HAIS-Q Average Score for Part 2
Blue	5.23	5.84
Gold	5.71	5.9
Green	5.12	5.62
Orange	5.16	5.68

Table 1. The average HAIS-Q score for each True Colors self schema for part 1 and part 2. The increase in information security is significant (p-value is 0.47).

Score	zxcvbn	Our Criteria
Zero	0	0
One	29	11
Two	100	65
Three	85	107
Four	40	66
Five	0	7

Table 2. Number of passwords with scores 0–5 in our password criteria. Note that zxcvbn scores are only from zero to four.

self schemas. It is also worth noting that the Gold self schema has a much higher average score. This could be due to these participants to be more organized.

We performed a similar analysis for the password security knowledge questions and received a similar result. Overall, the scores improved, which shows that regardless of the message, the participants improved their password security knowledge. Messaging works. However, matching vs mismatching messages did not have any significant difference. This could be because the first part of the message already tells the participant what constitutes a strong password.

4.6. Comparison of Password Strengths Scores

Password strength scores were calculated using zxcvbn. We now explore if a different metric would yield better insights. Table 2 shows the relationship between scores evaluated by zxcvbn and our metric of participant's passwords. Our metric looked at the password and awarded a point for each of the following: 1) a length greater than 8 characters, 2) a mix of numbers and letters, 3) including a special character, 4) a mix of upper and lower case characters, and 5) not including a dictionary word. The dictionary contains all the words from the English dictionary and words specific to the university such as the university name, mascot's name, etc. The maximum score that a password could receive was 5, and the minimum was 0. It can be seen from Table 2 that the passwords for zxcvbn and our criteria match pretty closely in terms of password strengths. The correlation between the two scores was calculated to be 0.801232, which shows that our criteria is closely

related to zxcvbn scores. This shows that our metric can be used to accurately evaluate password strengths in a simpler manner than zxcvbn.

5. Discussion and Limitations

Our results show that messaging had an effect in improving password security knowledge. However, targeted/matching messaging had a mixed result. This could be because the core part of the messaging is diluted as all participants learned what constitutes a strong password. Choosing a strong password or changing password security behavior might take longer to affect than just one month (length of time between completing part 1 and part 2 of the survey). Moreover, many of the participants had relatively high security knowledge score (e.g. the average HAIS-Q score was 5.3 out of possible 7).

Although the Big Five personality traits did not seem to have any effect on participants' chosen password, participants with the Green True Colors self schema tended to pick a stronger password. This is interesting result as personality studies are well-established. Could this mean that users with a certain personality are more likely to exhibit less secure (or more secure) behaviors? This could then be used for a more targeted and successful cybersecurity training by companies. Even though it is expected that information security knowledge would be a good predictor for security behaviors such as choosing a strong password, we found that this is not always the case. The information security knowledge could be too general or generic versus a more focused password security knowledge which seems to be a better predictor. This could mean that generic cybersecurity training might not be that effective but focused modules are needed.

In an enterprise setting, employees' self schemas can be easily obtained. In an online public setting, users' self schemas can be collected at account creation through a short survey. The advantage of using the True Colors self schema is that only one or two questions are needed.

Although there has been criticisms of personality types tests regarding their validity and reliability [42], [43–45] have shown that the True Colors self schema is valid and reliable. Other have shown that personality types have an effect: on learning [46], business coaching [47], and the type of software tasks preferred [48]. There have also been previous work [9, 49] that showed the effect of message effectiveness on advertising. Moreover [50] suggests that personalized messages may work better if participants are told explicitly that they are receiving a message based on their personality. This could be one possible explanation why our messages had minimal effect across personalities.

Password strength relies on resistance to brute force attacks and also dictionary and targeted attacks. Our password strength score includes dictionary and some targeted keywords. Both zxcvbn and our password score are shown to be highly correlated. Other password advice such as passphrases, using password managers, etc. could also have been given, but we wanted to give one short and clear message.

One limitation of our research is that most of the participants are college-age students. These participants are also considered to be part of the Gen-Z generation and might be more tech-savvy but less worried about privacy/security issues online. Regardless, this research shows promising results that personality does have an effect on security behaviors and matching messaging has the potential to be effective. Future research can expand on the participant pool, demographics, and diverse background.

Although we asked the participants to enter a password in part 2 of the survey, we told them in part 1 that they had to remember that password. It was not the goal of this research to measure whether participants remember passwords after one month. The point of asking them that question was to ensure participants would create a strong usable password. Only 105 participants entered a password in part 2; 18 of them were the same passwords, but 64 were similar (lowercase instead of uppercase or missing characters at the end). Thus, 78% of participants mostly remembered the password they entered in part 1. Thus, we could not measure if the matching message had an effect in the participants choosing a stronger password in part 2. Future work could ask participants to create a password they consider strong for a bank account but that is different from their current passwords.

6. Conclusion

We distributed an online survey and received 254 participants for the part 1 of the survey and 132 participants for the part 2 of the survey sent a month later. The survey consisted of questions asking about participants' self schemas, information security knowledge, and information security behavior. The survey also shows either a matching or mismatching message to each participant based on their True Colors self schema. It then asks the participant to create a password that they consider to be strong.

The results show that 66% of participants with a Green True Colors self schema picked a strong password, compared to less than 50% for the other True Colors self schemas. Green self schemas tend to be knowledgeable and competent. Participants who knew more about information security did not necessarily choose a stronger password. However, participants who knew more about password security and what

constitute a strong password, tended to pick a stronger password. The results also show that messaging works and can improve security behavior.

The relationship between self schema and information security, especially password security, need to be researched further. The True Colors self schema is currently marketed to corporations, governments, and schools [7]; thus, those who want to improve their IT security could take note of the differences in self schemas in password security. This could lead to more effective cybersecurity training for companies and for education. The effect of matching messages can also be studied in more depth by varying the messages work and considering the longitudinal effect of the messaging.

7. Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. DGE 1918591 and 1919004.

References

[1] Hebblethwaite, C. (accessed 2020), The average person has 7 social media accounts, https://marketingtechnews.net/news/2017/nov/17/average-person-has-7-social-media-accounts/.

[2] Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. *et al.* (2010) Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10 (New York, NY, USA: Association for Computing Machinery). doi:10.1145/1837110.1837113, URL https://doi.org/10.1145/1837110.1837113.

[3] Bryant, K. and Campbell, J. (2006) User behaviours associated with password security and management. *Australasian Journal of Information Systems* **14**(1). doi:10.3127/ajis.v14i1.9, URL https://journal.acs.org.au/index.php/ajis/article/view/9.

[4] Tan, J., Bauer, L., Christin, N. and Cranor, L.F. (2020) Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*: 1407–1426.

[5] Farcasin, M. and Chan-tin, E. (2015) Why we hate it: two surveys on pre-generated and expiring passwords in an academic setting. *Security and Communication Networks* **8**(13): 2361–2373. doi:10.1002/sec.1184, URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1184.

[6] Rothmann, S. and Coetzer, E.P. (2003) The big five personality dimensions and job performance. *SA Journal of Industrial Psychology* **29**(1). doi:10.4102/sajip.v29i1.88, URL https://sajip.co.za/index.php/sajip/article/view/88.

[7] Colors, T. (accessed 2020), The four color personalities: True colors intl.: Personality assessment training, http://www.truecolorsintl.com/the-four-color-personalities/.

[8] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017) Individual differences and information security awareness. *Computers in Human Behavior* **69**: 151–156.

[9] Brock, T.C., Brannon, L.A. and Bridgwater, C. (1990) Message effectiveness can be increased by matching appeals to recipients' self-schemas: Laboratory demonstrations and a national field experiment. *Emotion in advertising: Theoretical and practical explorations* : 285–315.

[10] Miller, M.M. and 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)**: 27–312.

[11] York, V.K., Brannon, L.A. and Miller, M.M. (2012) Increasing the effectiveness of messages promoting responsible undergraduate drinking: Tailoring to personality and matching to context. *Health Communication* **27(3)**: 302–309.

[12] York, V.K., Brannon, L.A. and Miller, M.M. (2012) Marketing responsible drinking behavior: Comparing the effectiveness of responsible drinking messages tailored to three possible 'personality' conceptualizations. *Health Marketing Quarterly* **29(1)**: 49–65.

[13] Pilling, V.K. and 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.

[14] Pease, M.E., Brannon, L.A. and Pilling, V.K. (2006) Increasing selective exposure to health messages by targeting person versus behavior schemas. *Health Communication* **19(3)**: 231–240.

[15] Brannon, L.A. and McCabe, A.E. (2002) Schema-derived persuasion and perception of aids risk. *Health Marketing Quarterly* **20(2)**: 31–48.

[16] Florencio, D. and Herley, C. (2007) A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07 (New York, NY, USA: Association for Computing Machinery): 657–666. doi:10.1145/1242572.1242661, URL https://doi.org/10.1145/1242572.1242661.

[17] Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T. *et al.* (2012) How does your password measure up? the effect of strength meters on password creation. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12 (USA: USENIX Association): 5.

[18] Christin, N., Egelman, S., Vidas, T. and Grossklags, J. (2012) It's all about the benjamins: An empirical study on incentivizing users to ignore security advice. In Danezis, G. [ed.] *Financial Cryptography and Data Security* (Berlin, Heidelberg: Springer Berlin Heidelberg): 16–30.

[19] Herley, C. (2009) So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09 (New York, NY, USA: Association for Computing Machinery): 133–144.

doi:10.1145/1719030.1719050, URL https://doi.org/10.1145/1719030.1719050.

[20] Gaw, S. and Felten, E.W. (2006) Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06 (New York, NY, USA: Association for Computing Machinery): 44–55. doi:10.1145/1143120.1143127, URL https://doi.org/10.1145/1143120.1143127.

[21] Dashlane (Accessed 2020), https://www.dashlane.com/.

[22] LastPass (Accessed 2020), https://www.lastpass.com/.

[23] PasswordSafe (Accessed 2020), https://pwsafe.org/.

[24] zxcvbn (2017), Dropbox zxcvbn, https://github.com/dropbox/zxcvbn.

[25] van Thiel, E. (accessed 2020), What are the big five personality test traits? - learn all about the theory, https://www.123test.com/big-five-personality-theory/.

[26] Myers, I.B. and Myers, P.B. (1995) *Gifts Differing: Understanding Personality Type* (Palo Alto, Calif.: Davies-Black Pub), 2nd ed.

[27] Foundation, T.M..B. (Accessed 2020), https://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/.

[28] Bravo-Lillo, C., Cranor, L.F., Downs, J. and Komanduri, S. (2011) Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* **9**(2): 18–26.

[29] Egelman, S., Cranor, L.F. and Hong, J. (2008) You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08 (New York, NY, USA: Association for Computing Machinery): 1065–1074. doi:10.1145/1357054.1357219, URL https://doi.org/10.1145/1357054.1357219.

[30] Weirich, D. and Sasse, M.A. (2001) Pretty good persuasion: A first step towards effective password security in the real world. In *Proceedings of the 2001 Workshop on New Security Paradigms*, NSPW '01 (New York, NY, USA: Association for Computing Machinery): 137–143. doi:10.1145/508171.508195, URL https://doi.org/10.1145/508171.508195.

[31] Redmiles, E.M., Liu, E. and Mazurek, M.L. (2017) You want me to do what? a design study of two-factor authentication messages. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (Santa Clara, CA: USENIX Association). URL https://www.usenix.org/conference/soups2017/workshop-program/way2017/redmiles.

[32] Lastdrager, E., Gallardo, I.C., Hartel, P. and Junger, M. (2017) How effective is anti-phishing training for children? In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17 (USA: USENIX Association): 229–239.

[33] Cialdini, R.B. and Ascani, K. (1976) Test of a concession procedure for inducing verbal, behavioral, and further compliance with a request to give blood. *Journal Of Applied Psychology* **61(3)**: 295–300.

[34] Cialdini, R.B., Wosinska, W., Barrett, D.W., Butner, J. and Gornik-Durose, M. (1999) Compliance with a request in two cultures: The differential influence of social proof and commitment/consistency on collectivists and individualists. *Personality And Social Psychology Bulletin* **25(10)**: 1242–1253.

[35] Petrova, P.K., Cialdini, R.B. and Sills, S.J. (2007) Consistency-based compliance across cultures. *Journal Of Experimental Social Psychology* **43(1)**: 104–111.

[36] Adams, A. and Sasse, M.A. (1999) Users are not the enemy. *Commun. ACM* **42**(12): 40–46. doi:10.1145/322796.322806, URL https://doi.org/10.1145/322796.322806.

[37] Maraj, A., Martin, M.V., Shane, M. and Mannan, M. (2019) On the null relationship between personality types and passwords. *2019 17th International Conference on Privacy, Security and Trust (PST)* .

[38] Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018) Correlating human traits and cyber security behavior intentions. *Computers & Security* **73**: 345 – 358. doi:https://doi.org/10.1016/j.cose.2017.11.015, URL http://www.sciencedirect.com/science/article/pii/S0167404817302523.

[39] Gross, T., Coopamootoo, K. and Al-Jabri, A. (2016) Effect of cognitive depletion on password choice. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2016)*: 55–66.

[40] Halevi, T., Lewis, J. and Memon, N. (2013) A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web*, WWW '13 Companion (New York, NY, USA: Association for Computing Machinery): 737–744. doi:10.1145/2487788.2488034, URL https://doi.org/10.1145/2487788.2488034.

[41] Scoresheet, M.M.B.F. (Accessed 2020), https://psychology.okstate.edu/faculty/jgrice/psyc4333/MiniMarkersScoresheet.pdf.

[42] Pittenger, D.J. (1993) Measuring the mbti... and coming up short. *Journal of Career Planning and Employment* **54**(1): 48–52.

[43] International, T.C. (2013), https://truecolorsintl.com/wp-content/uploads/2013/05/Research-Validity-and-Reliability-I.pdf.

[44] Crews, T.B., Bodenhamer, J. and Weaver, T. (2010) Understanding true colors personality trait spectrums of hotel, restaurant, and tourism management students to enhance classroom instruction. *Journal of Teaching in Travel & Tourism* **10**(1): 22–41. doi:10.1080/15313220903558538, URL https://doi.org/10.1080/15313220903558538. https://doi.org/10.1080/15313220903558538.

[45] Randall, R., Ferguson, E. and Patterson, F. (2000) Self-assessment accuracy and assessment centre decisions. *Journal of Occupational and Organizational Psychology* **73**(4): 443–459.

[46] Fatahi, S., Kazemifard, M. and Ghasem-Aghaee, N. (2009) Design and implementation of an e-learning model by considering learner's personality and emotions. In *Advances in electrical engineering and computational science* (Springer), 423–434.

[47] Harper, A. (2008) Psychometric tests are now a multi-million-pound business: what lies behind a coach's decision to use them? *International Journal of Evidence*

Based Coaching & Mentoring .

[48] Capretz, L.F., Varona, D. and Raza, A. (2015) Influence of personality types in software tasks choices. *Computers in Human behavior* **52**: 373–378.

[49] Brannon, L.A. and Brock, T.C. (1994) Test of schema correspondence theory of persuasion: Effects of matching an appeal to actual, ideal, and product 'selves'. *Attention, attitude, and affect in response to advertising* : 169–188.

[50] 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.