Personality Types and Passwords

Anna Bakas, Spencer Johnston, Eric Chan-Tin, and Shelia Kennison (OSU)

Preparing people to lead extraordinary lives

Abstract

- People often create passwords for their accounts that are insecure and then reused across multiple platforms => This leaves users vulnerable to hackers
- Different users have different personality types:
  - Big Five: openness, conscientiousness, extraversion, agreeableness, and neuroticism
  - TrueColors: orange, brown, green, and blue
- Participants with a green personality type tend to pick stronger passwords
- Participants, who agree that stronger passwords should be used regardless of convenience, chose weaker passwords
- Participants mostly understand what makes a strong password, even if they do not use one

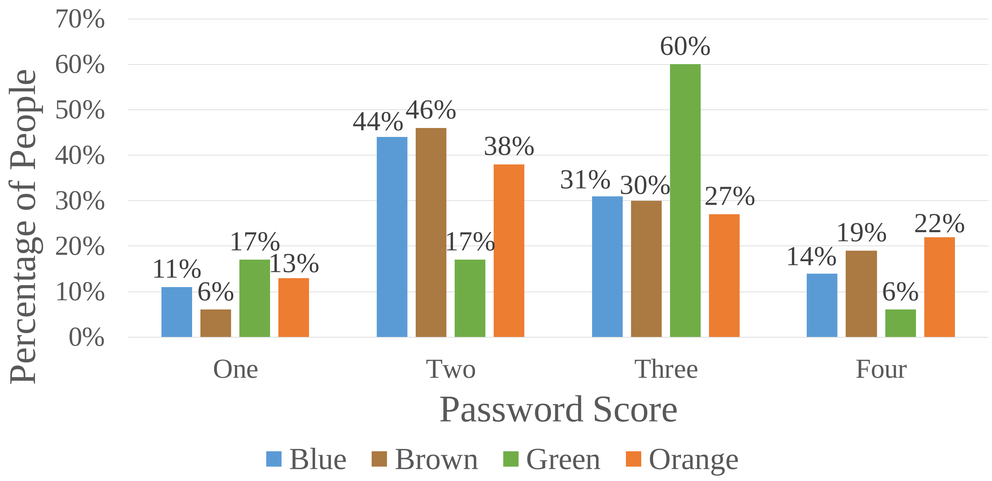
Background

- TrueColors Personality Types
  - Orange: energetic, spontaneous, charming
  - Brown: punctual, organized, precise
  - Green: analytical, intuitive, visionary
  - Blue: empathetic, compassionate, cooperative
- Zxcvbn software [1] provides a password score
  - 0: Too guessable: risky password.
  - 1: Very guessable: protection from throttled online attacks.
  - 2: Somewhat guessable: protection from unthrottled online attacks.
  - 3: Safely unguessable: moderate protection from offline slow-hash scenarios.
  - 4: Very unguessable: strong protection from offline slow-hash scenarios.

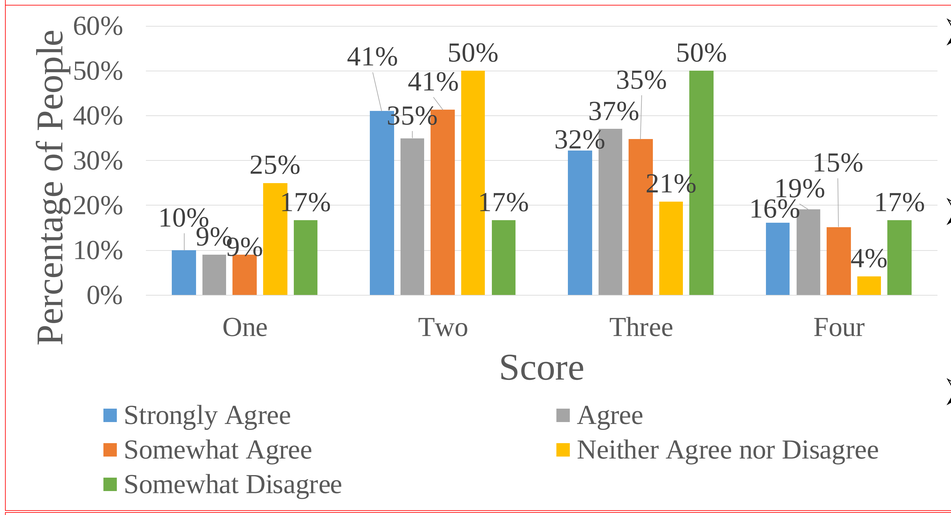
Research Design

- Qualtrics survey recruiting students from the SONA system
- Fall 2019
- Survey included questions covering personality types, social media use, demographics, and some questions regarding password usage
- One question asked the participants to write a password they consider to be strong
- 254 people participated in the survey

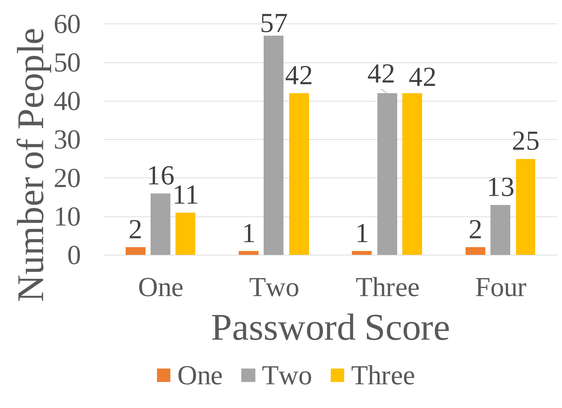
Results



- The figure shows the TrueColor personality type and their password scores, breaking down how many participants for each personality type picked a particular password score.
- No participant wrote a password that was given a password score of 0.



- The user was asked whether strong passwords ensure that accounts are safe and harder to hack into, even if they are inconvenient to use
- Participants who strongly disagreed with this statement had weaker passwords than those who strongly agreed.
- Disagree and Strongly Disagree only had one user choose them, so that data has been omitted



- Users were asked a series of questions:
  - How many characters a strong password has?
  - Do strong passwords include uppercase letters?
  - Do strong passwords include numbers?
- Their answers were then assigned a score and totaled with a minimum score of zero and a maximum score of three (no one scored a zero)
- The bars represent how many people scored what value based on their password score

Discussion

- Some personality types are more likely to pick insecure password => more targeted training can be performed to improve the cybersecurity awareness of these people.
- More targeted training could lead to better return on investment and lower number of successful attacks.

Acknowledgements

- This research was approved by the university's IRB.
- This material is based upon work supported by the National Science Foundation under Grant No. DGE-1919004 and DGE-1918591

References

- [1] Dan Wheeler, Dropbox, Inc., zxcvbn [Computer software]. Retrieved from https://github.com/dropbox/zxcvbn