*Preparing people to lead extraordinary lives*

# Personality Types, Passwords, and Cybersecurity Nudges

Anna Bakas, Anne Wagner, Eric Chan-Tin, and Shelia Kennison (OK State)

## 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 True Colors self schema tended to pick a stronger password
- Participants had relatively high security knowledge score
- Messaging had an effect in improving password security knowledge

## 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.

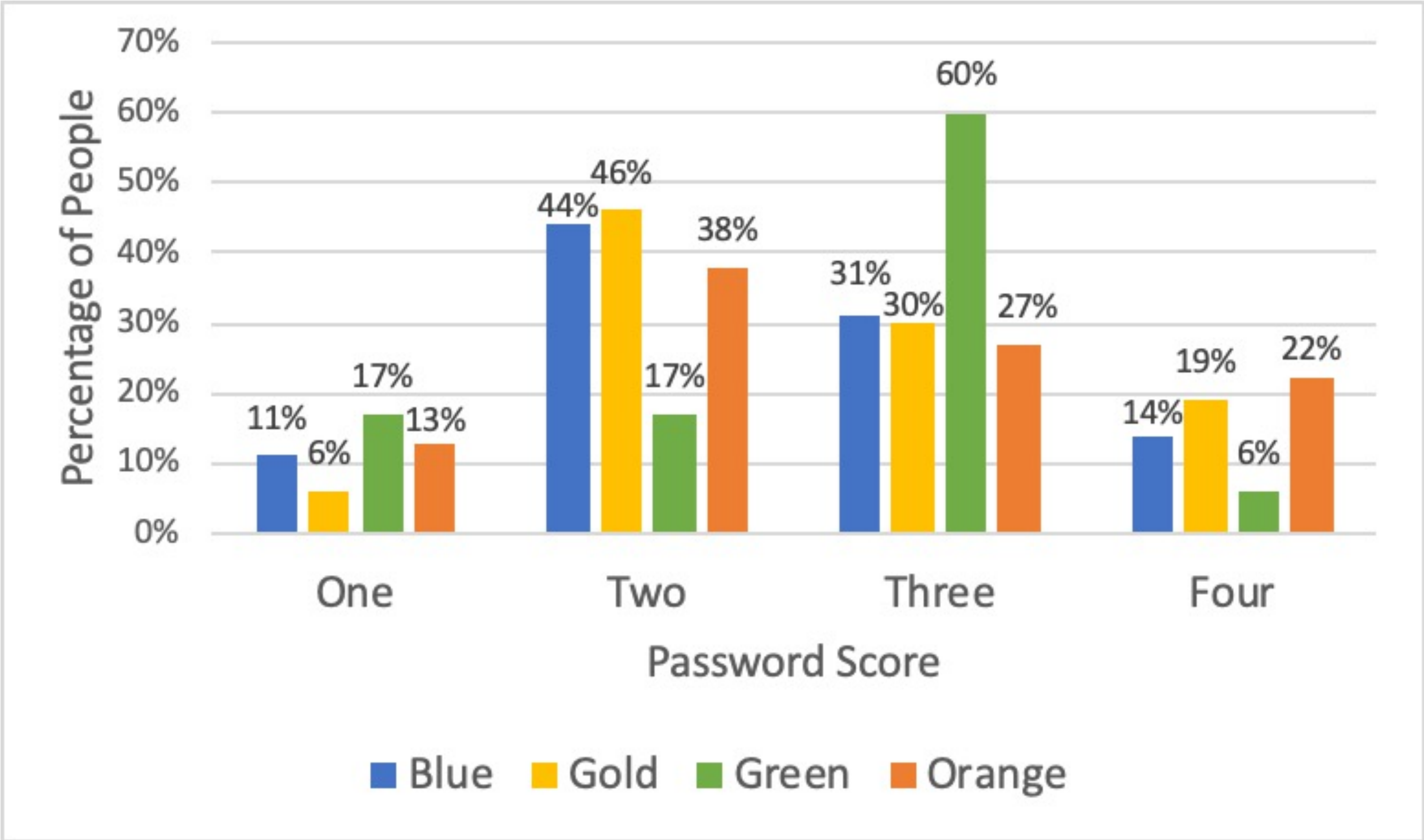
## Research Design

- Qualtrics survey recruiting students from the SONA system during Fall 2019
- Two parts: Part 2 was a month later
- 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

| 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 |

- Users were asked to complete the Human Aspects of Information Security Questionnaire (HAIS-Q), which consists of 9 questions. It includes questions such as:
  - “It's acceptable to use my social media passwords on my work accounts.”
- Each question was rated on a 7-point Likert with the points value being reversed for some questions.
- This figure shows the average HAIS-Q score for each self schema for both part 1 and part 2.
- The score increased for all self schemas.
- The Gold self schema has a higher average score.
- The improved scores shows that regardless of the message, the participants improved their password security knowledge. Messaging works.
- For those participants shown a matching message, their average score increased from 5.31 in part 1 to 5.78 in part 2.



- 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.
- There is a higher percentage of people with a green personality to select a password with password strength score of three

## Discussion

- Some personality types are more likely to pick insecure password => more focused training modules can be performed to improve the cybersecurity awareness of these people.
- Targeted/matching messaging works to some extent => more time needed to change password security behavior

## Acknowledgements

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

## References

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