Personality Types and Passwords

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

Abstract
- People often create passwords for their accounts that are insecure and then reused across multiple platforms which 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.

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.

Discussion
- Some personality types are more likely to pick insecure passwords, so 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