Personalized Cybersecurity Education and Training

DGE-1919004 and DGE-1918591

D. Eric Chan-Tin (Loyola University Chicago) chantin@cs.luc.edu

Shelia Kennison (Oklahoma State University) shelia.kennison@okstate.edu

Overview

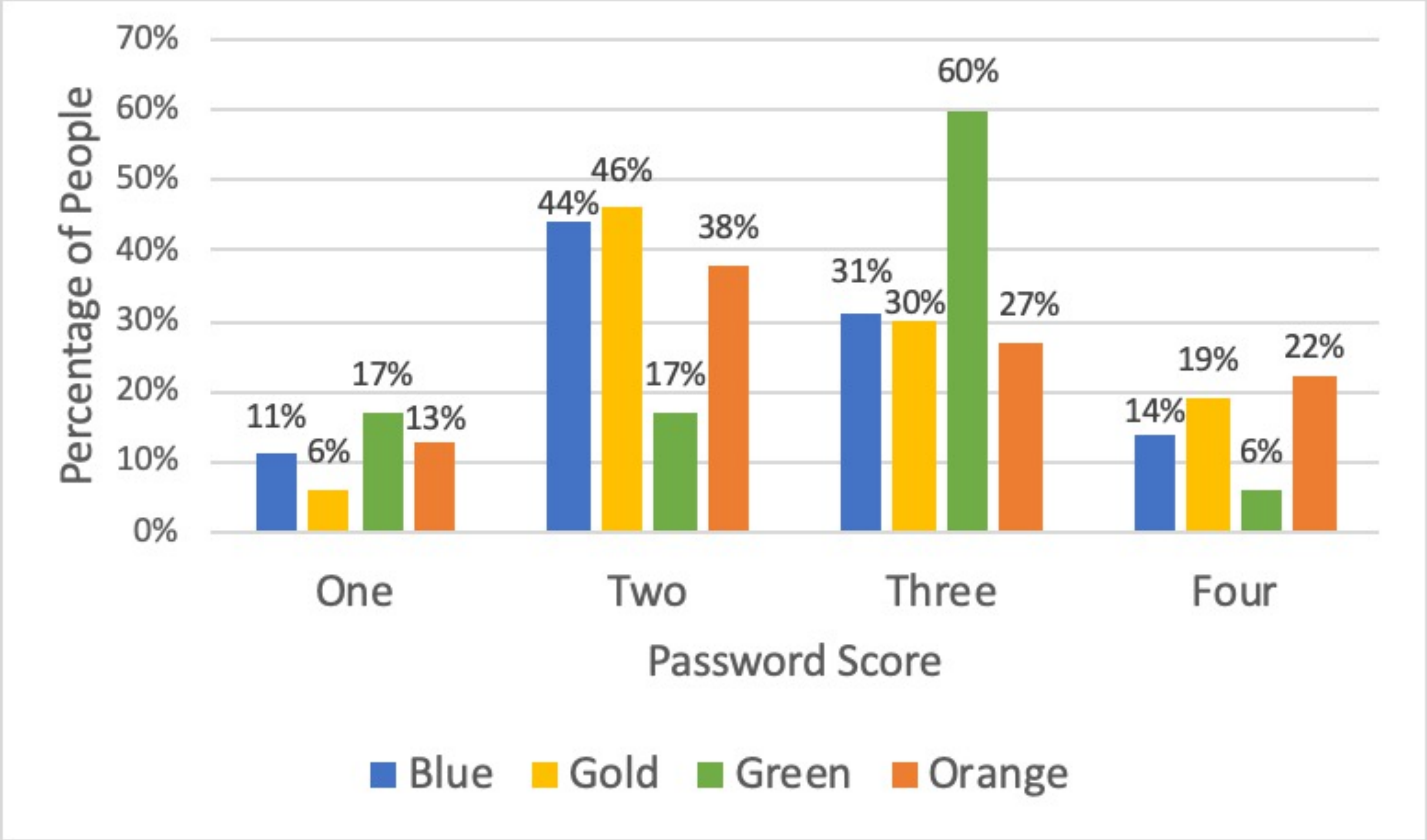
Current cybersecurity education and training are not effective.

Need for tailored cybersecurity education and training because there is no one-size-fits-all approach

Focus on two cybersecurity topics:

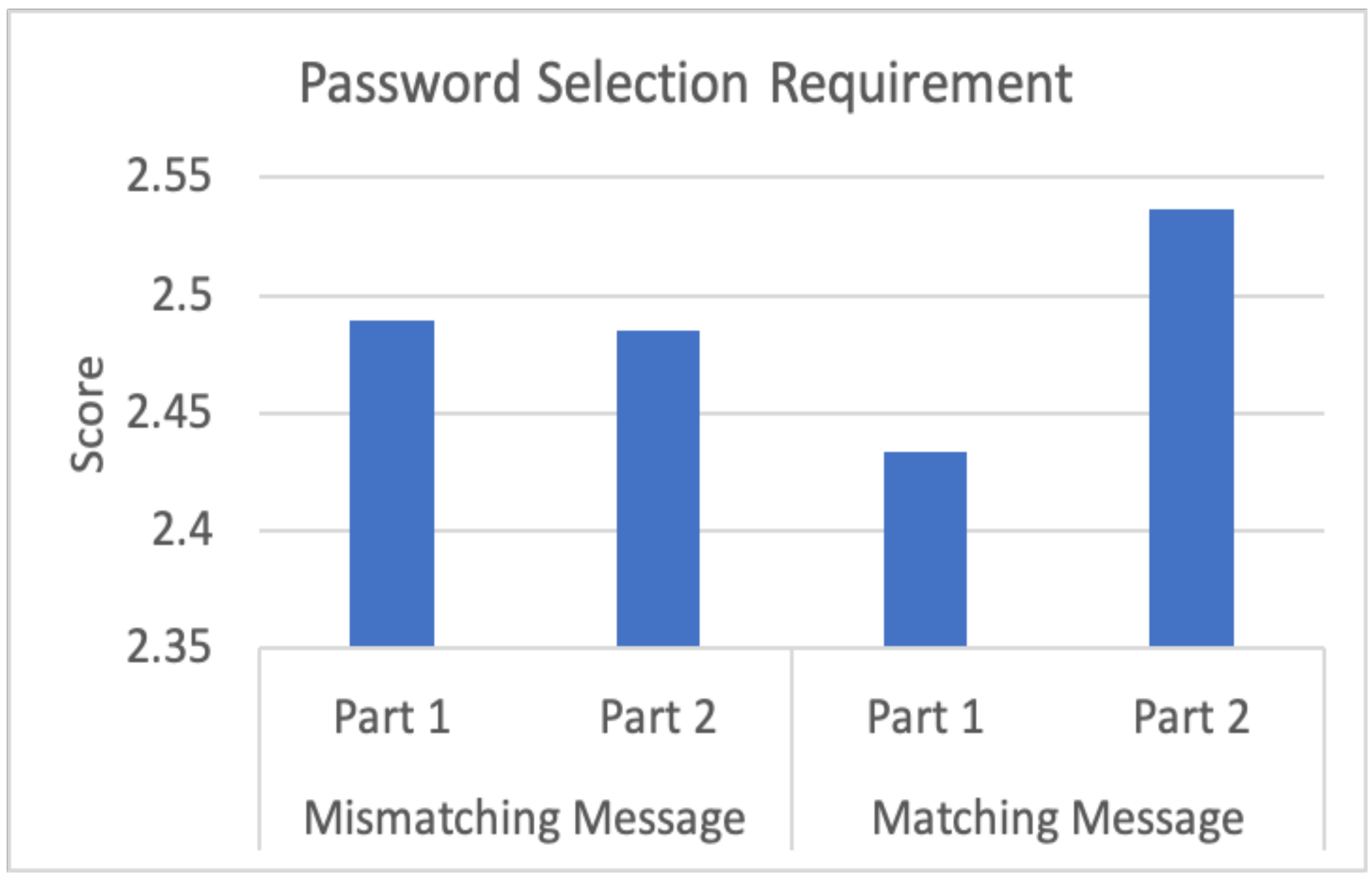
- Password creation/management
- Phishing

Relation between personality and password strength



Scientific Impact

- Cybersecurity behaviors can be changed!



Password Creation

Survey on personality styles, cybersecurity knowledge, and password creation

Matching or mismatching message to improve password strength

Survey 2 on cybersecurity knowledge and password creation after 1 month

Survey 3 on cybersecurity knowledge and password creation after 6 months

Phishing

Survey on personality styles, decision-making, vulnerable strategies, protective strategies, and prior victimization

Phishing email on

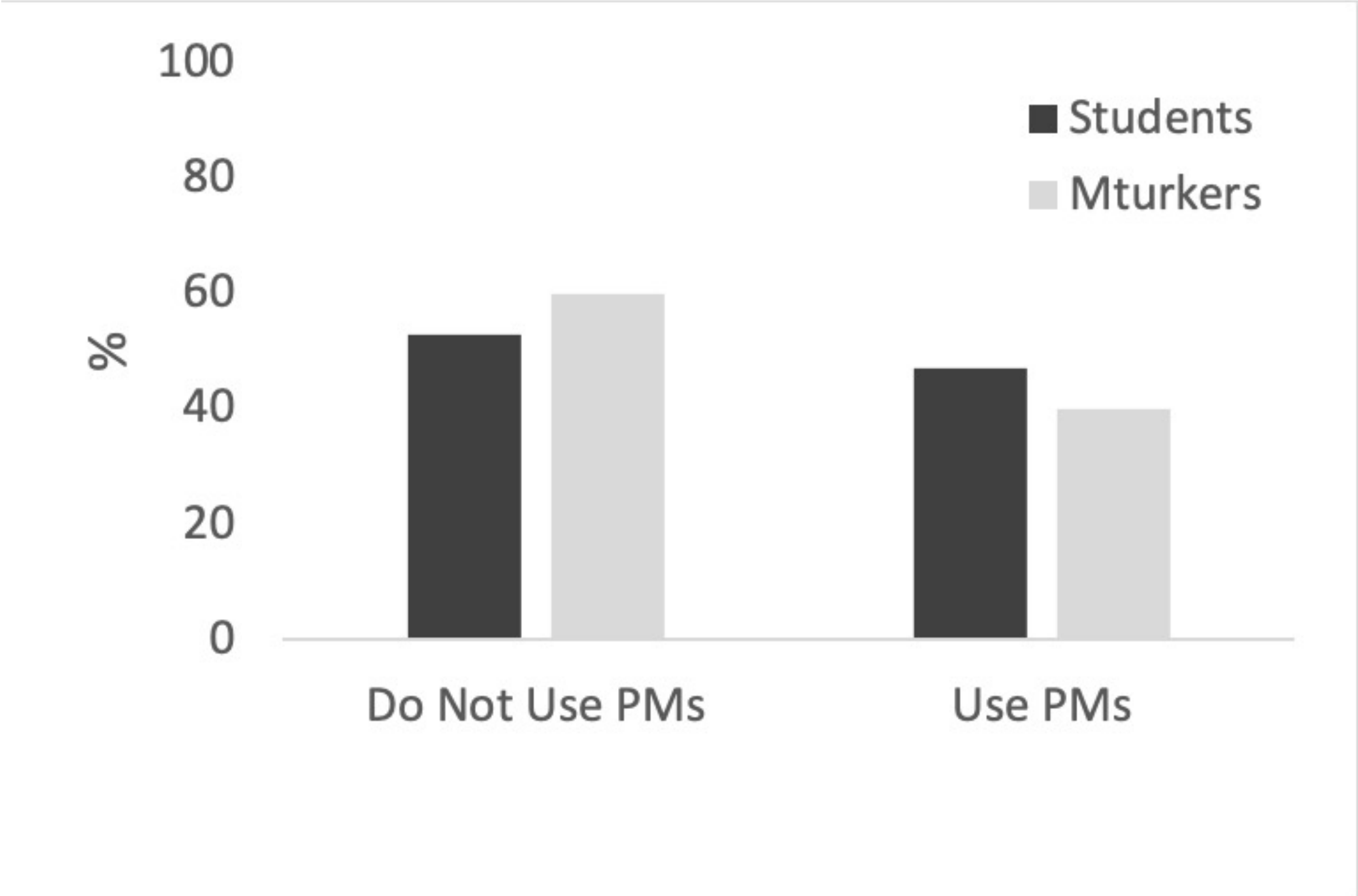
1. Charity (pragmatic, normative, altruism)
2. Locked account (authority)
3. Covid Lottery

Individuals with stronger systematic decision-making style were *less likely* to be phished

Individuals with low avoidant decision-making styles were more likely to be phished

Also: they were more likely to have high generalized anxiety

Few participants are using Password Managers (PMs)



Broader Impacts

- More effective cybersecurity education => decrease in attack success rate
- Applications to public health and business training

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting)
June 1-2, 2022 I Arlington, Virginia