Security Choice Task: Balancing Effort and Concern in Password Selection

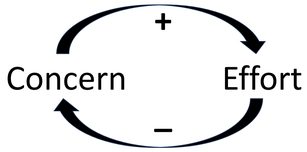
Nicholas Major[1], David Braun[2] & Catherine Arrington[1] [1]*Lehigh University* [2]*Drexel University*

#6013

Background

In a world full of password updates and dual authentication, how do individuals make choices about cybersecurity?

Two psychological constructs that may influence security choices are effort and concern.



Effort

Mental effort is the delegation of cognitive resources toward a task and individuals consider the costs and benefits of exerting effort (Kool & Botvinick, 2018).

People are cognitive misers, seeking to minimize mental effort (Fiske & Taylor, 1984).

Concern

Psychological concern arises from threat appraisals of the likelihood and severity of harm (Sulaiman et al., 2022).

Concern for online security and privacy is linked to technology adoption and implementation (Udo, 2001).

Predictable relationships between effort and concern should play into individual choices about securing cyber-systems.

Current Research

Goal: Develop a new paradigm that manipulates and measures factors associated with effort and concern in a simple lab analogue or model task of cybersecurity environments.

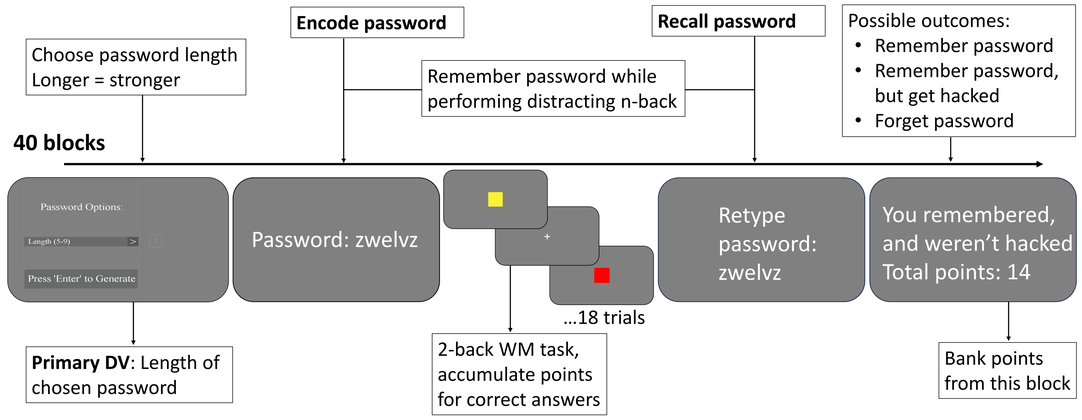
Elements of the Security Choice Task:

- Choose password strength
- Memorize automatically generated password
- Perform n-back task & accumulate points
- Remember password

Cover Story:
"In this game you will be **collecting points** for your performance on a **visual memory task** and placing them in a 'bank.' Your goal across the experiment will be to collect as many points as you can, so your performance on the memory task matters. At the end of each round, you will be able to pull your points out of a temporary bank and add them to your total. However, getting those points out of the bank requires that you **remember your password** and that **your bank was not hacked**. The chance of a hack varies based on **how secure your password is**. You will be making **choices about how strong you want your password** to be in terms of length and complexity in each round of the game."

Methods

Structure of the Security Choice Task



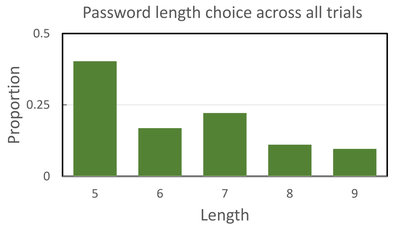
Task Considerations

- **Piloting questions:**
  - How can we optimize the parameters of the task:
    - What are the best password length and complexity boundaries?
    - How does n-back difficulty influence password memory?
  - **Overall:** What parameters lead to participants remembering passwords ~70% of the time?
- **Questions about effort:**
  - How are password lengths and complexities related to memory performance?
  - Does password efficacy influence willingness to exert effort when making password choices?
- **Questions about concern:**
  - How do changes to the likelihood or severity (i.e., how many points can be lost) of a hack influence password choices?

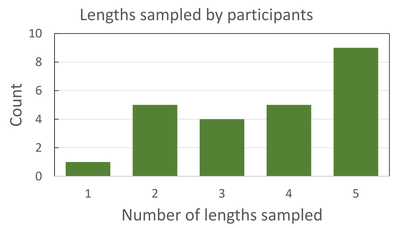
Results

Password Behavior

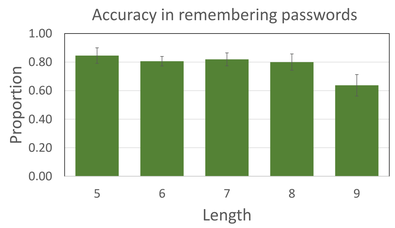
Was there variability in password choice?



Did participants choose different lengths?



How well were passwords recalled?

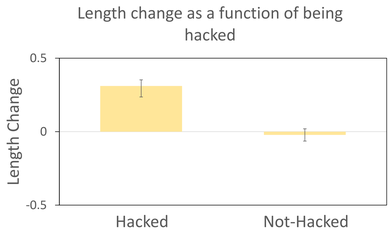


Influences on Choice

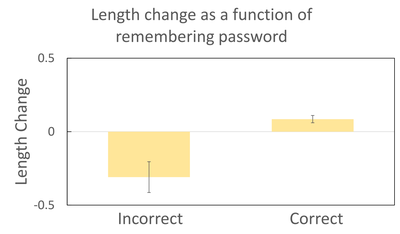
Does the outcome of the most recent block influence password choice in line with predictions about effort and concern?

Length change
password length on the previous block *minus* password length on the current block

Did getting 'hacked' influence password choices?



Did forgetting passwords influence password choices?



Conclusions/Future Directions

This paradigm may allow us to capture security choices in a lab analogue of a cybersecurity environment.

- Across and within participants variability of password choices occurred, allowing us to test for systematic changes in cybersecurity choices.
- Based on recent outcomes, participants made choices aligned with predictions based on effort and concern.
- **Future directions**: Does changing the likelihood and severity of a hack (i.e., password efficacy or size of reward) influence password choices? Will changing the effort of recalling passwords (i.e., through complexity of symbol type) influence password choice?

Contact information: Nick Major – njm224@lehigh.edu; Kate Arrington – kate.arrington@lehigh.edu