ReSCIND Performer HSR Dataset Cover Sheet

ReSCIND

Dataset Details

Dataset Title:	CASPAR Stage 1 HSR, Silver Tier Behavioural Tasks ("Funfair")		
Dataset Citation:	TBD		
Data Format:	Text files (CSV, XML)	Data Size:	< 5 MB
Dates & Duration:	Sep 30 2024 – Jun 30 2025 Approx 1hr per participant.	Time Zone:	All of them.
How to access dataset:	https://osf.io/wm39e/		
Point of Contact for data questions:	Email Scott Brown scott.brown@newcastle.edu.au		

Description of Scenario

Experiment Objectives

This data set is one of three parts in HSR aimed at evaluating efficacy of cognitive biases in reducing the productivity of cyber attackers. This one of the three parts ("Funfair", or "Silver Tier") implements measurements of cognitive biases in behavioral tasks which are based in established methods from the cognitive science literature, but with procedural adjustments to align them with ecologically valid cyber behaviors (as measured in the "Gold Tier" part of the experiment).

Experiment Description

Data collection completely online. Different pools of participants sourced from undergraduate students (no cyber expertise) and also from online networks of cyber experts. Silver Tier data collection occurred after participants completed consent procedures, a skills test, and then the "Gold Tier" cyber experiment (a capture-the-flag style HSR). In the Silver Tier data collection, participants spent approximately 1 hour in several different lab-style behavioral tasks. These tasks were presented as games of chance and skill in "funfair" environment, with established cognitive tasks hidden within. For example, there was a "lottery" game in the funfair which instantiated a standard behavioral risky choice paradigm, and a "slot machine" game which instantiated a standard behavioral task measuring the near miss effect. The experiment was written in JavaScript. Deployment and data security were handled via JATOS.

Experimental Results

Full details of the experimental results are available in our Data Report (email for access). Briefly, the experiments showed that standard behavioral measures of cognitive biases could be replicated in an online funfair environment, and that these could be aligned with cyber-relevant versions of the same biases. Measurements were taken for the following biases: Law of Small Numbers; Gambler's Fallacy; Hot Hand Effect; Endowment Effect; and the Sunk Cost Fallacy. Measurements of the size of the bias agreed (within error margins) with corresponding measurements in the Gold Tier cyber experiment for the Law of Small Numbers, the Endowment Effect, and the Sunk Cost Fallacy.

Data

Data Sources

Primary Data Sources

Each of the behavioral tasks in the funfair environment recorded data to secure servers via JATOS. Those data are available in raw form as specified by JATOS (JSON-like, see details here: https://www.jatos.org/JATOS-Results-Archive-JRZIP.html). These primary data include logs of all relevant events – keypresses, mouse clicks, display contents, etc.

Derivative Data Sets

Data were processed from the raw format into formats suitable for analysis with R and Python. The data sets available for download include Jupyter Notebooks which detail this process. The high level goal was to create uniformly rectangular long-format tables of relevant events, and then subsequently summarized versions of these which focus on relevant independent and dependent variables, per person per condition. All elements of this processing are documented carefully in the Notebooks.

Alongside the cleaned, processed, derivative data set for each cognitive bias, users will find a data dictionary. The dictionary is generated via the Jupyter Notebook which processes data for that bias, and the dictionary is also saved out separately as a CSV, which provides easy access for users who are not interested in Jupyter Notebooks. Inside the Notebook, code cells and associated text cells explain the dependent variables at a higher level. These explanations are in terms of psychological constructs, including definitions of correct/incorrect responses. Summaries of these are included in the data dictionary CSV files (under "caption" column name).

Research

Hypotheses

These data were used to investigate the hypothesis that cognitive biases could be measured in behavioral tasks adapted from established methods to more closely align with cyber-relevant tasks. These data were subsequently used to investigate the hypothesis that the measured bias would agree in magnitude (within error limits) with measurements of the same bias from the corresponding cyber-relevant task.

Publications

French, L., Thorpe, A., Salibayeva, K., Brown, S., Eidels, A., Forties, R., Fry, Z., Hewlett, E., & Inoue, H. (2024). *Combatting cyberattacks with cognitive bias*. [Conference presentation]. Performance and Expertise Research Centre Conference, Sydney, Australia.

Thorpe, A., French, L., Salibayeva, K., Brown, S., Eidels, A., Forties, R., Fry, Z., Hewlett, E., & Inoue, H. (2025). *Hackers are (only) human too: Understanding cognitive biases in cybersecurity* [Conference presentation]. Australasian Mathematical Psychology Conference, Sydney, Australia.

French, L., Thorpe, A., Salibayeva, K., Brown, S., Eidels, A., Forties, R., Fry, Z., Hewlett, E., & Inoue, H. (2025). *Hackers are (only) human (part) too: Validating and exploiting biases to disrupt hacker efficiency* [Conference presentation]. Australasian Mathematical Psychology Conference, Sydney, Australia.

This will be updated as the project continues. The data set is reported in several publications which are currently either under review or in preparation.