# Evaluating the Applicability of Analyzing Phishing Email Judgments with the Double System Lens Model

Kylie Molinaro[1,2] and Matthew L. Bolton, Ph.D.[2]

[1]Johns Hopkins University Applied Physics Laboratory, [2]University at Buffalo

## Introduction

Phishing emails are a serious and continually growing threat to cybersecurity. There is a real and urgent need to understand what information humans use when making judgments about whether or not to trust an email so that phishing emails can be appropriately combated. We apply judgment analysis (JA) to phishing email judgments. Because JA has not been applied to this domain, this effort assessed whether or not the statistical assumptions of JA with multiple linear regression are upheld.

## Background

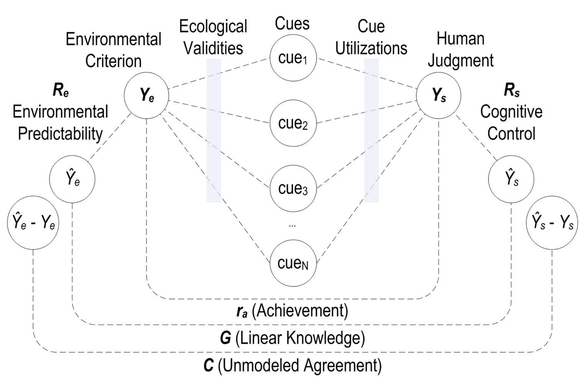
### HUMAN MODELS OF PHISHING JUDGMENT

- Suspicion, cognition, automaticity model [1]
- Signal detection theory [2]
- Mental modeling approach [3]
- These approaches do not evaluate how a person synthesizes information in their judgments

### JUDGMENT ANALYSIS

- Technique for analyzing how people make judgments of distal criteria (the environment) using proximal cues (information in the environment)
- Double system lens model: uses symmetric statistical models of the environment and the judgment values made by the human to evaluate human judgment
- Affords numerous analysis capabilities

$$r_a = GR_eR_s + C\sqrt{1-R_e^2}\sqrt{1-R_s^2}$$




*Graphical representation of the double system lens model.*

### PHISHING CUES

❖ **Technical Cues**
- URL Hyperlinking*
- Attachment Type
- Sender Display Name and Email Address

❖ **Visual Presentation Cues**
- No Branding/Logos*
- Poor Overall Design/Formatting

❖ **Message Language and Content Cues**
- Spelling and Grammar Errors*
- Generic Greeting*
- Use of Time Pressure/Threats*
- Use of Emotional Appeals
- Lack of Signer Details*
- Too Good to be True Offers*
- Requests for Personal Information*

* - used in our lens model analyses

## Methods

### EXPERIMENTAL TASK AND PARTICIPANTS

- Participants sorted 40 emails (20 legitimate and 20 phishing) into “keep” or ”suspicious” folders
- 10 student participants, average age of 23.2 years, six male and four female, five native English speakers

### APPARATUS

- PC or mobile smartphone with Roundcube (web-based email client) was used to interact with the emails

### INDEPENDENT VARIABLES AND EXPERIMENTAL DESIGN

- PC and mobile smartphone experimental conditions
- Dichotomous criterion: 1 for phishing, 0 for legitimate
- Dichotomous cue coding: 1 for present, 0 for absent

### DEPENDENT MEASURE

- Judgment the participant made about an email: 1 if sorted into “suspicious”, 0 if sorted into “keep”

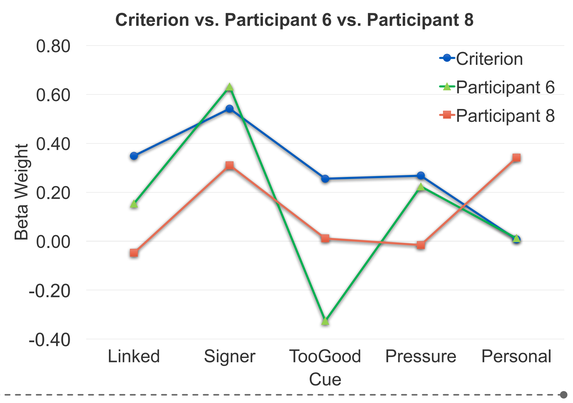
### DATA ANALYSIS

- Link-based phishing emails only: 20 legitimate and 18 phishing in total
- Cognitive Systems Engineering Educational Software used for double system lens model analyses [4]
- Eight cues in final lens model analyses (noted by * above)

## Results

| | Regression Models | | | | | | | | | Lens Model Statistics | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $\beta_0$ | $\beta_{Spelling}$ | $\beta_{Greeting}$ | $\beta_{Linked}$ | $\beta_{Branding}$ | $\beta_{Personal}$ | $\beta_{Signer}$ | $\beta_{TooGood}$ | $\beta_{Pressure}$ | | $R_e$ | | |
| Criterion | -0.510 | 0.033 | 0.194 | 0.349 | 0.400 | 0.007 | 0.542 | 0.255 | 0.268 | | 0.923 | | |
| Participant | | | | | | | | | | $r_a$ | $R_s$ | G | C |
| 1 | 0.175 | 0.475 | -0.009 | -0.106 | 0.040 | 0.309 | 0.223 | -0.045 | 0.262 | 0.789 | 0.840 | 0.834 | 0.679 |
| 2 | -0.226 | 0.141 | 0.265 | 0.322 | 0.106 | -0.225 | 0.387 | -0.272 | 0.383 | 0.669 | 0.771 | 0.897 | 0.138 |
| 3 | -0.038 | 0.556 | -0.060 | 0.101 | -0.065 | 0.341 | 0.301 | -0.584 | 0.105 | 0.760 | 0.877 | 0.834 | 0.460 |
| 4 | 0.127 | 0.419 | 0.024 | -0.129 | -0.087 | -0.121 | 0.490 | 0.087 | -0.018 | 0.709 | 0.792 | 0.861 | 0.342 |
| 5 | -0.510 | 0.033 | 0.194 | 0.349 | 0.400 | 0.007 | 0.542 | 0.255 | 0.268 | ~1.000 | 0.923 | ~1.000 | ~1.000 |
| 6 | -0.216 | 0.077 | 0.060 | 0.154 | 0.172 | 0.012 | 0.632 | -0.326 | 0.224 | 0.851 | 0.841 | 0.960 | 0.511 |
| 7 | -0.510 | 0.033 | 0.194 | 0.349 | 0.400 | 0.007 | 0.542 | 0.255 | 0.268 | ~1.000 | 0.923 | ~1.000 | ~1.000 |
| 8 | -0.118 | -0.018 | 0.201 | -0.048 | 0.218 | 0.341 | 0.310 | 0.011 | -0.016 | 0.489 | 0.648 | 0.842 | -0.049 |
| 9 | 0.018 | 0.108 | 0.117 | 0.098 | 0.060 | 0.234 | 0.461 | 0.003 | 0.156 | 0.748 | 0.749 | 0.952 | 0.350 |
| 10 | 0.263 | 0.065 | 0.109 | -0.084 | -0.088 | -0.363 | 0.642 | 0.136 | 0.102 | 0.527 | 0.676 | 0.783 | 0.134 |

- Range of achievement values
- High $R_e$ and $R_s$ values indicate that the linear models did a good job of fitting both the environment and the human judges
- High $G$ values indicate that the linear models of the human judges generally matched the linear model of the environment
- Large range of $C$ values suggest that there are distinct individual differences between participants
- Beta weights all positive in the criterion model
- Lack of signer details, no branding/logos, and URL hyperlinking appear to be the most diagnostic
- Comparison of judgment strategies to each other and criterion




## Discussion

The results indicate the lens model can be used to evaluate phishing judgments. The best evidence for this is seen in the high $R_e$ and $R_s$ values. Varying achievement scores were also observed across participants consistent with their varying levels of performance in the judgment task.

### ANALYSIS CAPABILITIES

- Compare cue validities and utilizations: is there a mismatch between what cues are most diagnostic and what cues are being used?
- Compare judgment strategies of different humans to each other and to the environment model
- Training and design intervention applications

### LIMITATIONS

- Email distribution – consistent with prior phishing research
- Unknowns with PC/Mobile condition effects
- Use of multiple linear regression over logistic regression to handle dichotomous criterion, judgments, and cues

## References

1. A. Vishwanath, B. Harrison, and Y. J. Ng (2016), “Suspicion, cognition, and automaticity model of phishing susceptibility”
2. C. I. Canfield, B. Fischhoff, and A. Davis (2016), “Quantifying phishing susceptibility for detection and behavior decisions”
3. J. S. Downs, M. B. Holbrook, and L. F. Cranor (2006), “Decision strategies and susceptibility to phishing”
4. M. L. Bolton and E. J. Bass (2005), “Cognitive Systems Engineering Educational Software: Educational software addressing quantitative models of performance”

## Acknowledgements

The authors would like to thank Dr. Anton Dahbura and Dr. Xiangyang Li from the Johns Hopkins University Information Security Institute and Dr. Nathan Bos from the Johns Hopkins University Applied Physics Laboratory for allowing them to use the data collected under the National Science Foundation Award 1544493 for the work presented here.