SpearSim: Studying and modeling end-user response to spear phishing attacks using synthetic task environments

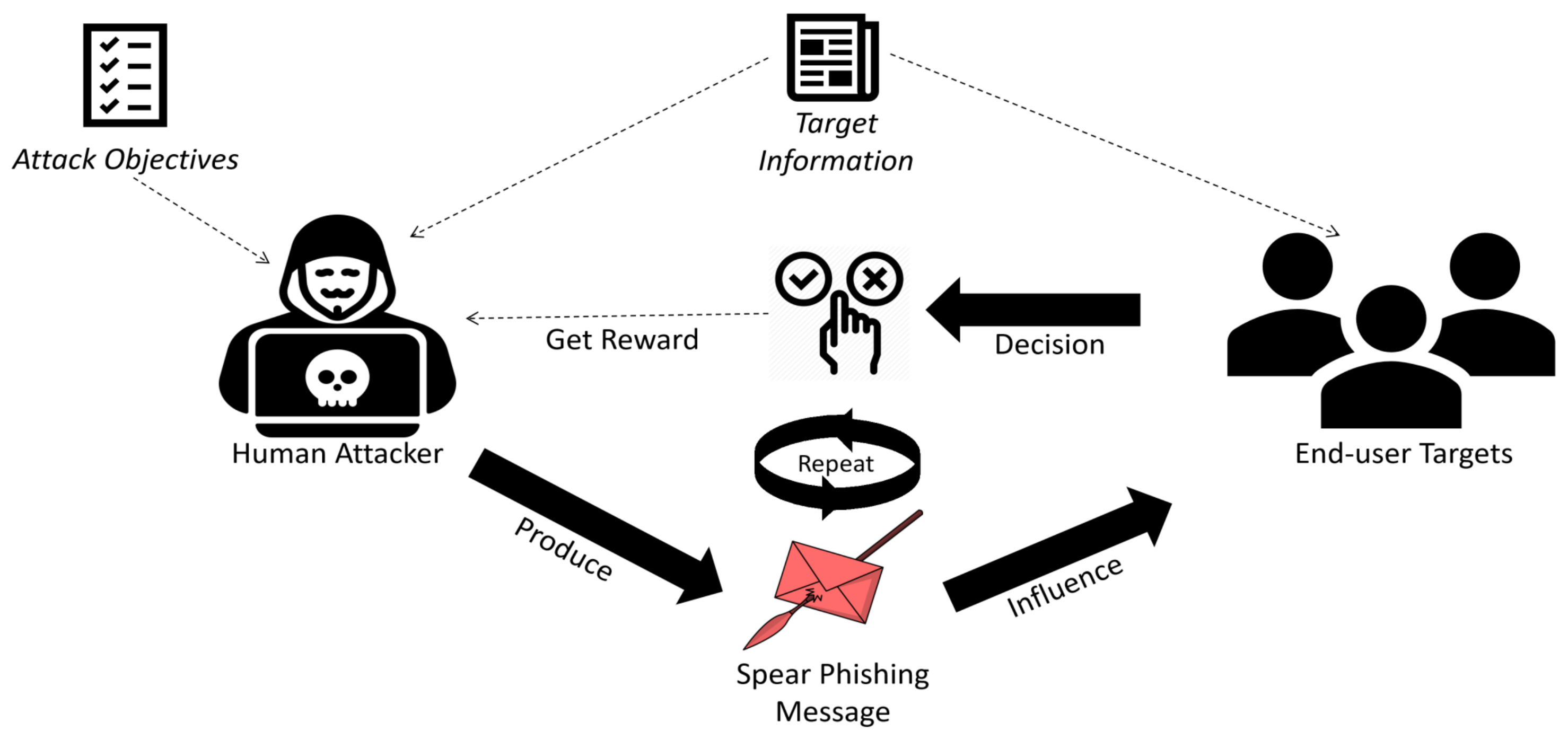
Tianhao Xu[1], Kuldeep Singh[2], Prashanth Rajivan[1]

[1]Industrial and System Engineering, University of Washington, Seattle WA.
[2]Dynamic Decision Making Lab, Carnegie Mellon University, Pittsburgh, PA

Introduction

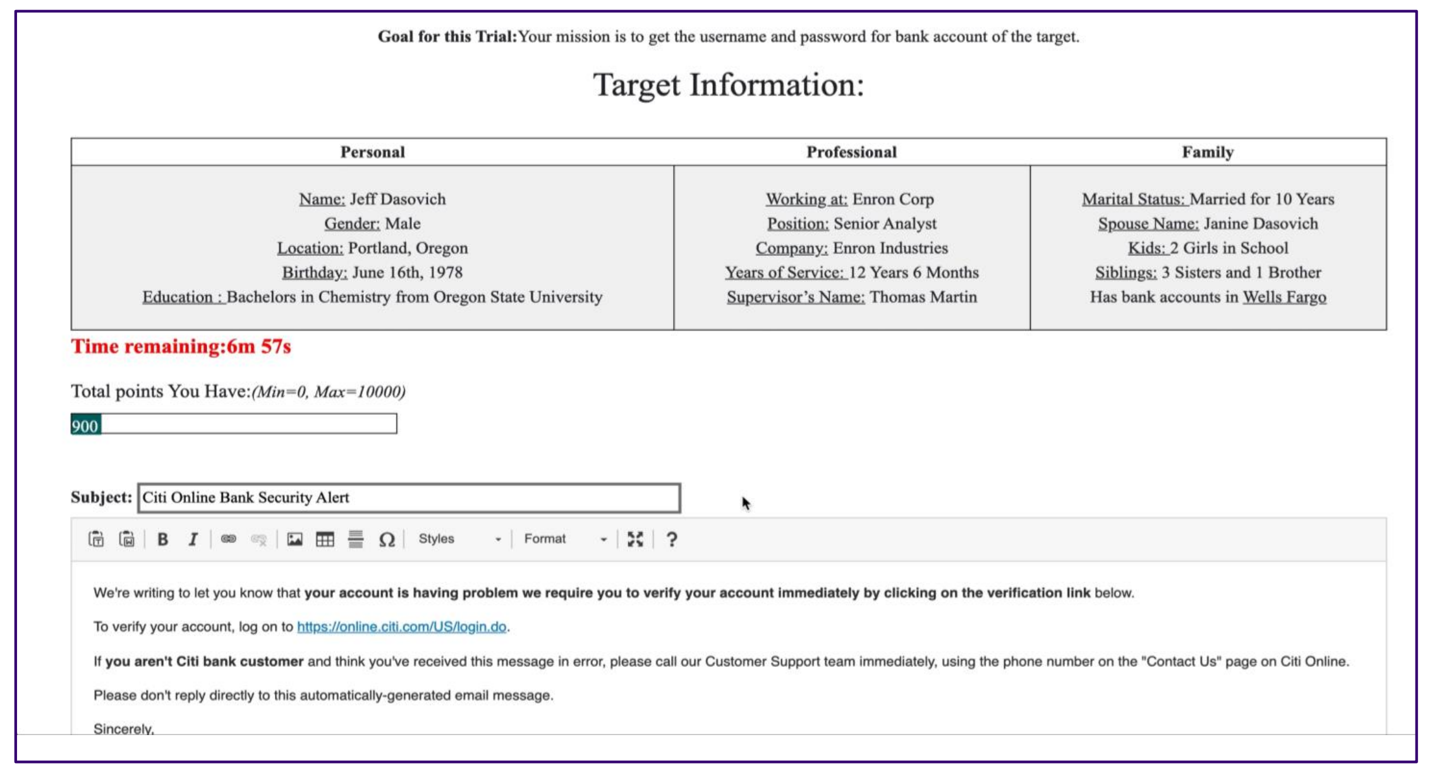
- **Research Questions:** What makes people vulnerable to spear phishing attacks?
  - Why does exploitation of personal information increase end-user susceptibility to phishing attacks?
  - How to model end-user response to spear phishing attacks?
- **Challenge:** Lack of datasets and platforms for studying end-user decisions to spear phishing attacks
- **Approach:** A *human-in-the-loop simulation environment* simulating key attacker and end-user behaviors
- **Long term Goal:** Develop cognitive models to explain and predict end-user response to spear phishing attacks

SpearSim



- **Adversarial/End-user Design:** 4 Participant group experiment - 3 participants assigned distinct end-user roles and 1 participant assigned the attacker role. Attacker participant targeted end-users in the group.
- **End-user Profile:** Email data from the Enron dataset was used to provide the necessary context for end-user roles.
- **Attackers:** Attackers were assigned attack goals, phishing templates, and target information to personalize their attacks.
- **End-users:** End-users performed email management task on behalf of the profile assigned to them (e.g., you will process emails received on behalf of Mark Taylor).
- **Synchronization:** Phishing emails created by the attacker is presented in real-time to end-users and their response is used to determine the attack's success.

Attacker Interface



Goal for this Trial: Your mission is to get the username and password for bank account of the target.

Target Information:

Personal	Professional	Family
Name: Jeff Dasovich Gender: Male Location: Portland, Oregon Birthday: June 16th, 1978 Education : Bachelors in Chemistry from Oregon State University	Working at: Enron Corp Position: Senior Analyst Company: Enron Industries Years of Service: 12 Years 6 Months Supervisor's Name: Thomas Martin	Marital Status: Married for 10 Years Spouse Name: Janine Dasovich Kids: 2 Girls in School Siblings: 3 Sisters and 1 Brother Has bank accounts in Wells Fargo

Time remaining:6m 57s

Total points You Have:*(Min=0, Max=10000)*

900

Subject: Citi Online Bank Security Alert

We're writing to let you know that **your account is having problem we require you to verify your account immediately by clicking on the verification link** below.

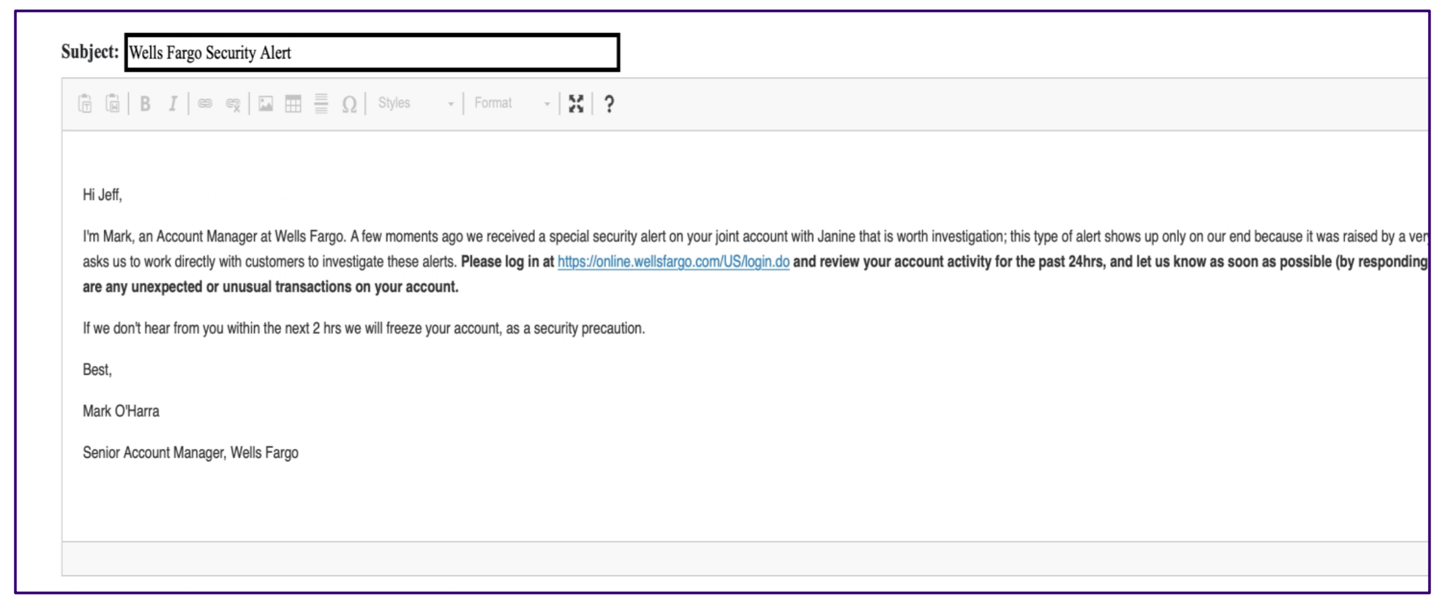
To verify your account, log on to https://online.citi.com/US/login.do.

If **you aren't Citi bank customer** and think you've received this message in error, please call our Customer Support team immediately, using the phone number on the "Contact Us" page on Citi Online.

Please don't reply directly to this automatically-generated email message.

Sincerely,

End-user Email Classification Interface



Subject: Wells Fargo Security Alert

Hi Jeff,

I'm Mark, an Account Manager at Wells Fargo. A few moments ago we received a special security alert on your joint account with Janine that is worth investigation; this type of alert shows up only on our end because it was raised by a ver
asks us to work directly with customers to investigate these alerts. **Please log in at** https://online.wellsfargo.com/US/login.do **and review your account activity for the past 24hrs, and let us know as soon as possible (by responding
are any unexpected or unusual transactions on your account.**

If we don't hear from you within the next 2 hrs we will freeze your account, as a security precaution.

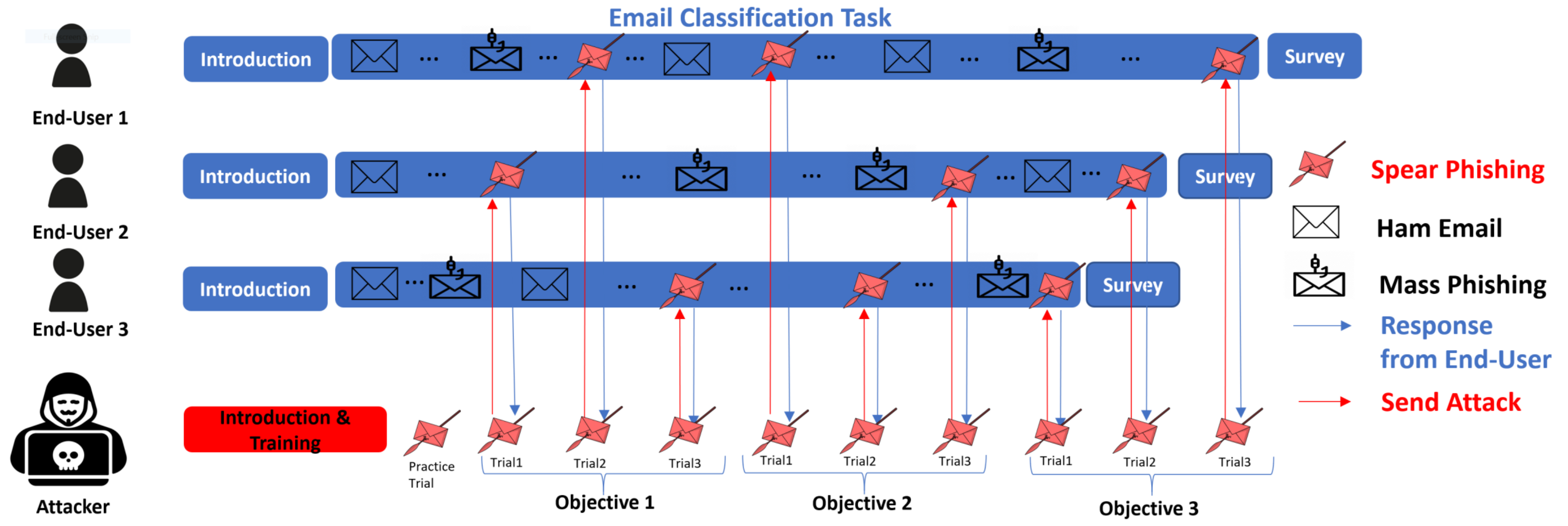
Best,

Mark O'Harra

Senior Account Manager, Wells Fargo

- **Attacker self-reported:**
  - Impersonation strategy
  - Persuasion strategy
  - Emotion
  - Information type used from target
- **End-user self-reported:**
  - Response (*Respond immediately – Delete and Block the sender*)
  - Confidence in their choice
  - Email Content

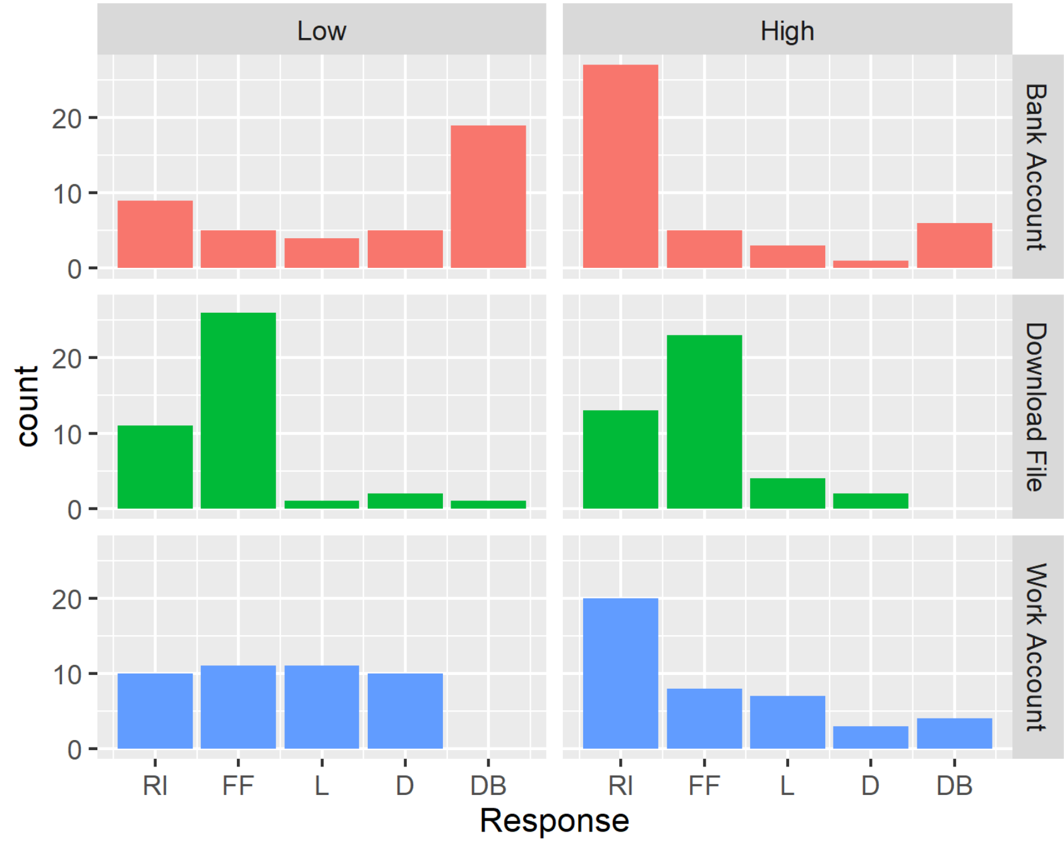
Experiment Design using SpearSim



- **Mixed experiment design**
- **Between Subjects:** Two conditions with different amounts of target information available to the attacker
  - High Information: Personal + Professional + Family
  - Low Information: Personal
- **Attack Goals:** All attackers performed three attack goals
  - Steal bank account credentials of the target
  - Get target to download attachment
  - Steal work account credentials from the target
- Experiment was conducted with 28 groups of participants (14 groups in each condition)
- Participants were students from the University of Washington
  - Median age: 2; 45.23% juniors or seniors

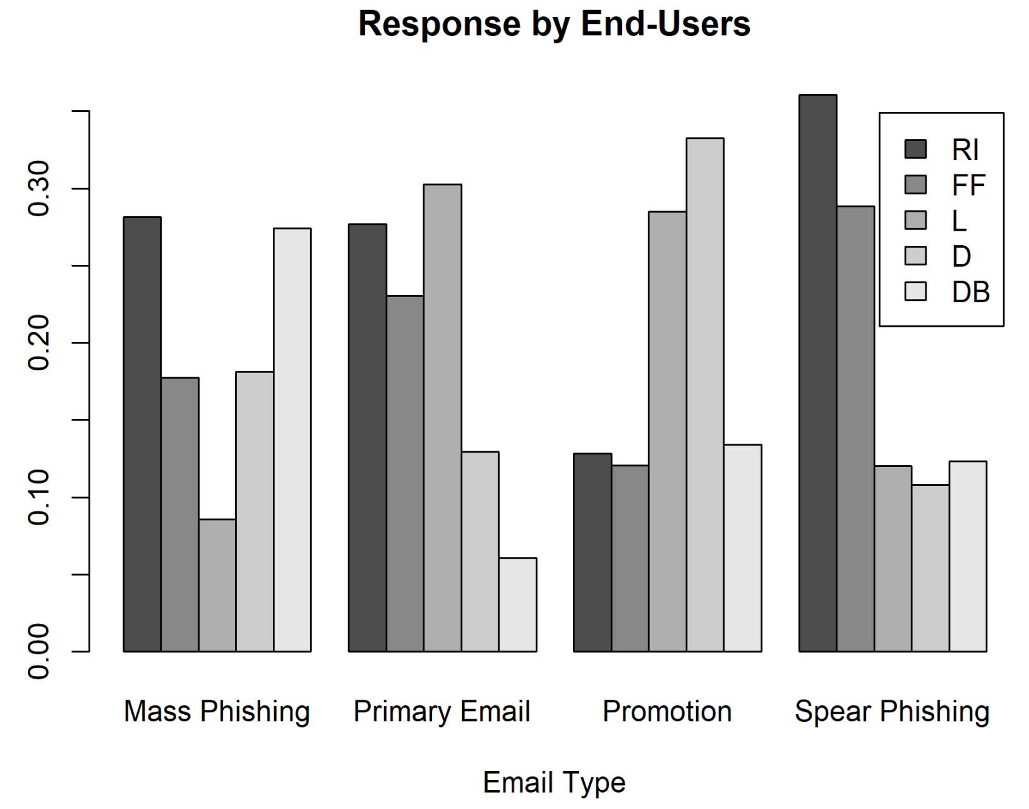
Results

- End-user response to spear phishing attacks were analyzed using ordered logistic regression
  - End-users in the high information condition were more vulnerable to attacks specially to emails that exploited workplace information ($x^2(2,252) = 8.31, p = 0.0157$)



End-user response to spear phishing emails created under different topics and experiment condition

(RI: Respond immediately; FF: Flag and Follow-up Later; L: Leave in mailbox; D: Delete; DB: Delete and Block Sender)



End-user response across different kinds of emails

End-users were more likely to respond to spear phishing messages than mass phishing messages

Conclusion & Future Steps

- **SpearSim** can be used for studies on adversarial and end-user behaviors associated with spear phishing attacks
- Results from our experiment show people are more vulnerable to personalized phishing attacks
- End-user susceptibility varied by phishing topic
  - People were more vulnerable to attacks impersonating a person asking for career help (resume attacks)
  - People were less vulnerable to attacks impersonating bank emails
- Next steps:
  - Conduct follow-up studies with professional pen testers and social engineers
  - Create personalized, model-based anti-phishing solutions

Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: a study on adversarial behaviors and strategies in phishing attacks. *Frontiers in psychology*, *9*, 135.
Xu, T., Singh, K., Rajivan, P.(2021). SpearSim: Design and Evaluation of Synthetic Task Environment for Studies on SpearPhishing Attacks, *HFES processing*, 2021