Building the Human Firewall:
Developing Organizational Resistance to Semantic Security Threats

Challenge:

What structures and incentives can organizations use to mitigate phishing attacks?

How can organizations support coordination among employees so they protect each other?

What is the best combination of interventions that organizations can use to combat phishing?

Solution:

Use crowdsourcing and gamification techniques to:

- Motivate reporting of phishing
- Increase accuracy
- Triage of new attacks

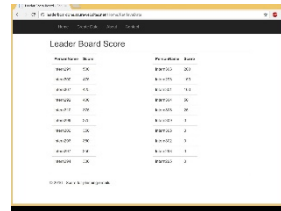Test versions of leaderboards and work disruption

NSF Project: #1421580

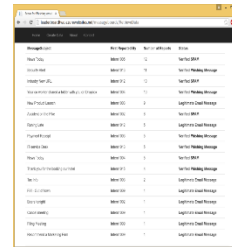**Matthew L. Jensen**, Univ. of Oklahoma, mjensen@ou.edu

Alexandra Durcikova, Univ. of Oklahoma, alex@ou.edu

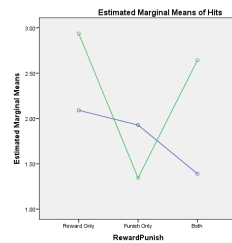**Ryan T. Wright**, Univ. Virginia, rtw2n@comm.virginia.edu

Individual-focused Leaderboard

Message-focused Leaderboard

More Hits

Fewer False Positives
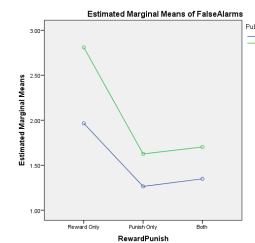
Variable	Best Focus
Number of Hits	**Phishing Message**
False positives	**Individual**
Work task	No difference
Motivation	**Phishing Message**
Anxiety	No difference
Paralysis	No difference
Phishing success	**Phishing Message** (17% vs. 28% individual focus)

Scientific Impact:

Attribution and feedback (rewards and punishments) produce:

- More hits
- Fewer misses

Public notification produces:

- More motivation
- Greater anxiety

No short-term disruption to productivity

Leaderboards focused on message more effective

Broader Impact:

Presentations and publications in academic venues

Disseminate to practitioners through:

- Presentations during industry meetings
- Meetings with industry leaders

Creation of training materials:

- Publically accessible
- In use at two organizations

Industry-oriented publications (e.g., cases and white papers)