

# Building the Human Firewall

PIs: Matthew Jensen, Alexandra Durcikova, Ryan Wright

casr.ou.edu

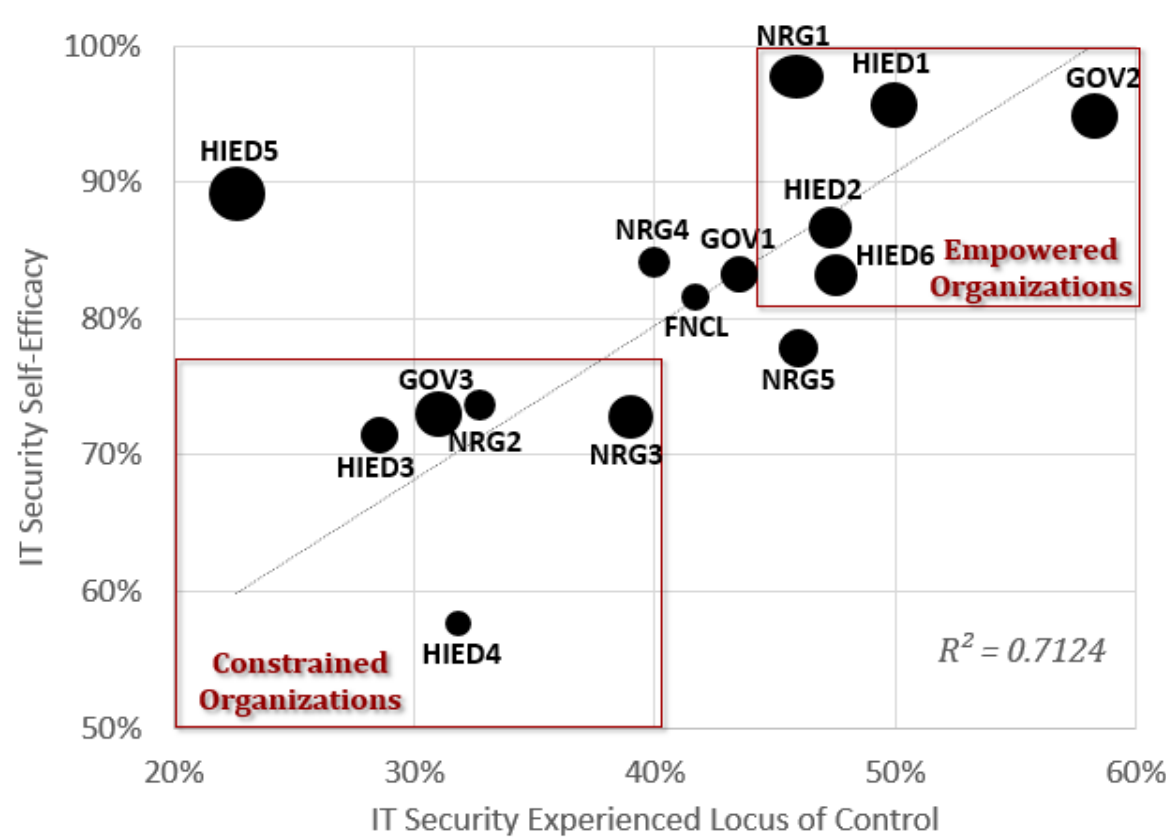
The objective of this project is to develop IT security strategies supporting organizations and individuals within organizations in combating phishing attacks.

## Supporting Organizations

**Data Source:** Interviews of managers of information security (or CISOs) from 15 organizations

**Data Analysis:** Each sentence in every interview was coded along the following dimensions: *Problem/Solution*, *Subject* (actor who was engaged), *Type of Response* (acquiescence, compromise, avoid, defy, and manipulate), *Tactics* (bridging, buffering).

**Findings:** IT security departments differ in terms of their locus of control (LOC) and self-efficacy (SE) about managing IT security threats; the two extreme sets of organization are *empowered* (high LOC and high SE) and *constrained* (low LOC and low SE). Second, organizational response (acquiescence, avoidance, compromise, and defiance) to bridging versus buffering by the IT Security function differs between constrained and empowered organizations.



**Locus of Control** = IT security subject / All subjects

**IT Security Self-Efficacy** = IT Security subject/ All subjects | given Solution (not Problem)

How can IT Security organizations get more support from their organizations at large?

	Bridging	Buffering
Empowered IT Security	✓	
Constrained IT Security		✓

**Bridging** = is the use of collaboration with multiple groups in an organizations to facilitate making compromises.

**Buffering** = is the act of persuading multiple groups of people by controlling important resources such as IT.

## Supporting Individuals

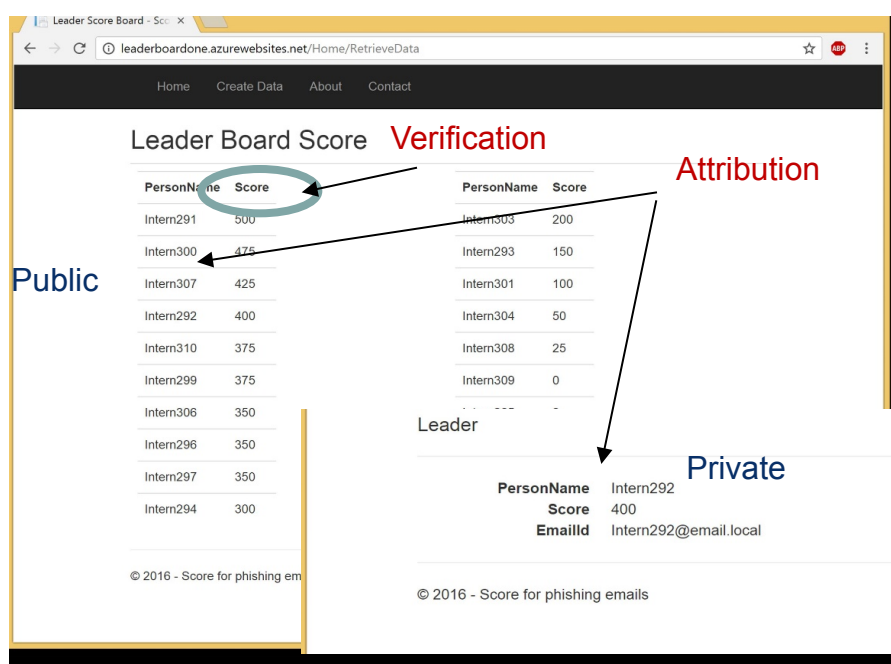
**Data Source:** Laboratory experiments with undergraduate students simulating work as an intern to a senior executive. Each participant was expected to accomplish work tasks and respond to work-related emails while watching for and reporting phishing messages (21 legitimate, 5 phishing).

**Experiment 1:** A 2 x 3 experiment crossing *Attribution* (public vs. private) and *Feedback* (rewards only vs. punishment only vs. both rewards and punishment) in a leaderboard. This treatment was further divided into two groups: competition (focus on individual) and cooperation (focus on phishing message) based gamification strategy executed through a leaderboard.

**Experiment 2:** A 2 x 2 x 2 experiment crossing *General Training* (presence/absence), *Just-In-Time Training* (rich/lean) and *Leaderboard* with both Attribution and Verification (present/absent) factorial experiment.

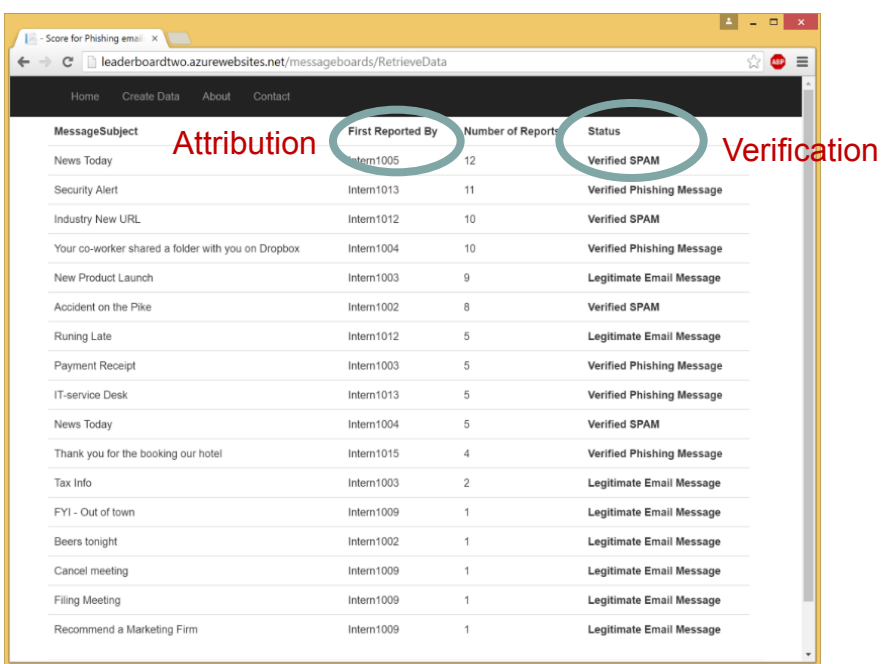
**Findings:** Attribution and Feedback must be used together to get the best outcome with respect to lower the success rate of phishing emails and to reduce anxiety and paralysis to the lowest possible values. Interestingly, the presence of leaderboards did not negatively influence the work task assigned to subjects. We observed that both general training and the presence of a leaderboard decreased the propensity to click on a phishing message, while we found no effect for different types of just-in-time training.

**Leaderboard - focus on individual**  
Competition as gamification strategy



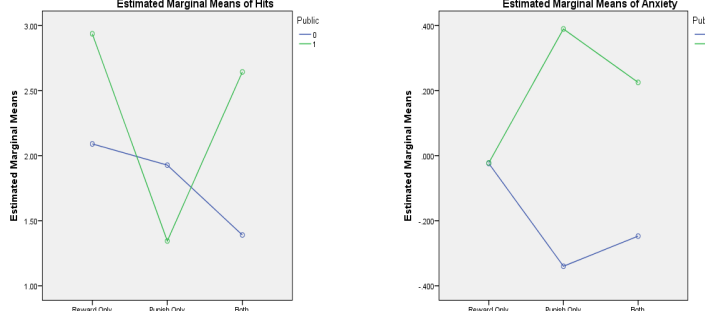
(N=171)

**Leaderboard - focus on phishing message**  
Cooperation as gamification strategy

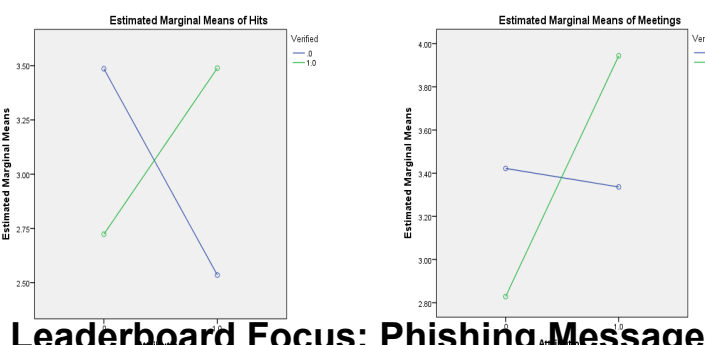


(N=104)

Dependent Variable	Leaderboard 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)



Leaderboard Focus: Individual



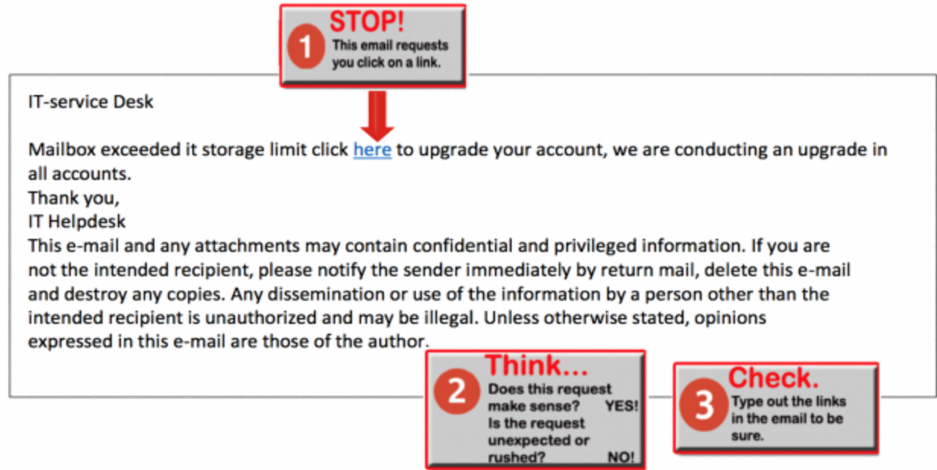
Leaderboard Focus: Phishing Message

**Example of Rich Just-In-Time Training**

**Message from the IT Security Team**

You have clicked on a phishing email that was sent out by PrepDesign IT Security Group. In the future please make sure you use the "Stop! Think. Check." Framework. For example see the mail you got below...

Please do NOT report this message to [phishing@email.local](mailto:phishing@email.local). You can now close this tab and continue with your work.



Experiment 1

Experiment 2

Independent Variable	Phishing success	No of Correctly Reported Phishing Messages
Just-In-Time Training (rich/lean)	No Difference	No Difference
General Training (present/absent)	Present (32% vs. 47%)	No Difference
Leaderboard (present/absent)	Present (31% vs. 49%)	No Difference
General Training X Leaderboard (both present/both absent)	Both Present (24% vs. 45%)	Both Present (Fewer messages are FWD)

Interested in meeting the PIs? Attach post-it note below!



National Science Foundation  
WHERE DISCOVERIES BEGIN

The 3<sup>rd</sup> NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting  
January 9-11, 2017  
Arlington, Virginia

