Research Proposal for the Cluster to Advance Cyber-Security and Testing (CAST)

Project Title: Design of Gamification for Information Security Awareness and Compliance: An Empirical Study in the Context of Phishing Emails

Bill Kettinger, Jong Lee and Chen Zhang,
Department of Business Information & Technology
Fogelman College of Business & Economics

Background

Phishing is a malicious attempt to trick people into revealing or sharing their sensitive personal information such as username, password, social security number, and credit card information by masquerading as a trustworthy person or organization using an electronic communication – most commonly emails (Ramzan 2010). In recent years, the number of unique types of phishing email attacks has steadily increased. For example, the Anti-Phishing Working Group (APWG) suggests that in the fourth quarter of 2014 there were 197,252 unique types of phishing attacks – an 18% increase from the third quarter of 2014 (Brownlee 2015). Falling victim to phishing email attacks can put individual users and their organizations at risk. For example, phishers can use personal data (e.g., username and password) to access a victim's financial account and withdraw money. Furthermore, phishers can potentially access sensitive organizational data such as financial data of customers and social security numbers of employees. Due to these potential consequences of phishing, most organizations educate their employees about phishing emails through training and urge them to notify the IT departments of phishing emails. Further, United States Computer Emergency Readiness Team (US-CERT) encourages web users to report phishing emails to US-CERT (phishing-report@us-cert.gov). While reporting phishing emails is an important source of collecting, analyzing, and exchanging information about verified credential collection sites used in phishing attacks, most employees tend to ignore or not bother to report phishing emails. Furthermore, security awareness training offered by organizations can be less effective in the long run as it tends to have only a short-term effect on employees' behavior and its long-term benefit for phishing prevention and reporting remains questionable. Motivated by this challenge, this research aims to determine the extent to which one can sustain users' vigilance to phishing by using gamification techniques to maintain user engagement. Specifically, the study will examine the impact of gamification design elements on sustaining phishing awareness, reporting, and prevention.

Justification for research

The objective of this proposed research is to empirically evaluate the conceptual model of how gamification design improves phishing reporting (figure 1), which was one of the major outcomes from the last year's CAST funded research project titled "Design of Gamification for Information Security Awareness and Compliance: A Conceptual Model of How Gamification Design Improves Phishing Reporting." Specifically, the proposed research project aims to build on previous year's project and empirically evaluate how gamification elements (relative performance feedback, small distance feedback, & permeability of class boundaries) influence employees' phishing email reporting behavior.

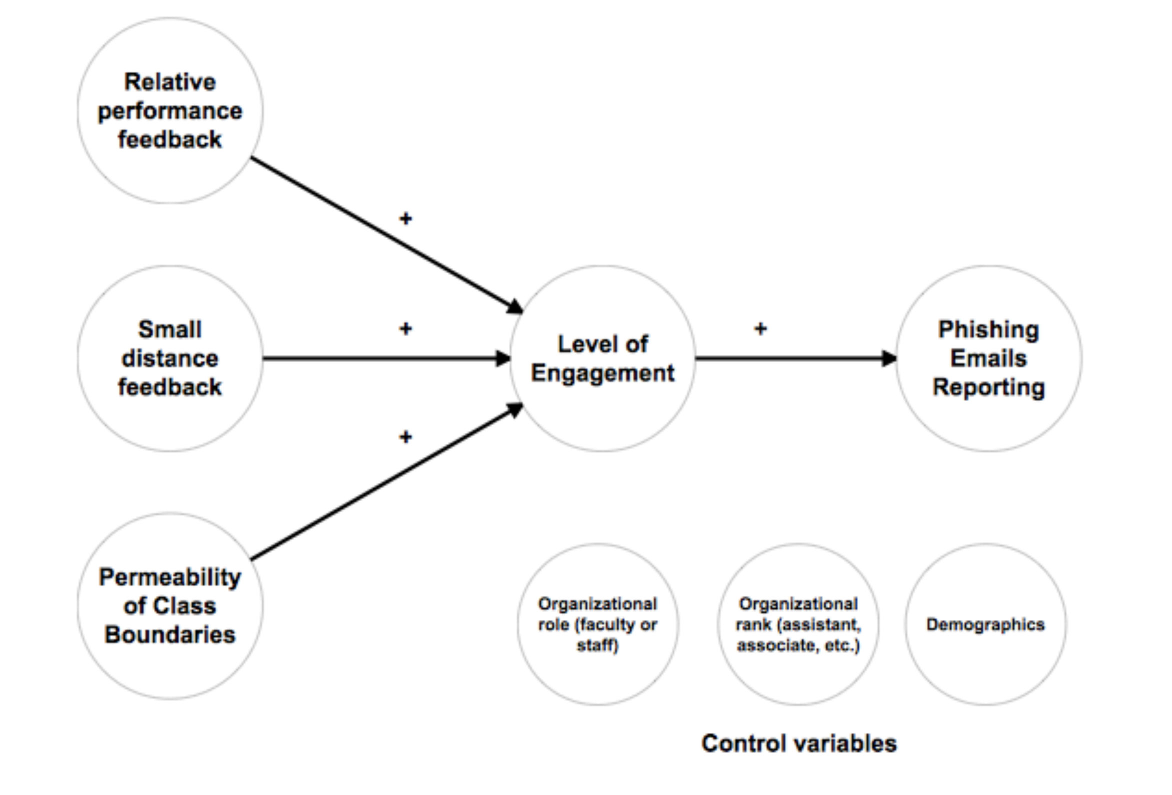
Relative performance feedback
Small distance feedback
Permeability of Class Boundaries
+
+
+
Level of Engagement
+
Phishing Emails Reporting
Organizational role (faculty or staff)
Organizational rank (assistant, associate, etc.)
Demographics
Control variables

Figure 1. Conceptual Model of How Gamification Design Improves Phishing Reporting

The proposed research will adopt an engaged scholarship approach and will involve collaborations with or support from regional companies, such as FedEx, and International Paper. Furthermore, we have had discussions and now have agreement with a leading anti-phishing solutions provider, PhishMe, to provide us with access to their phishing software platform and reporting tools for the project. Lastly, our empirical study will be conducted at the University of Memphis with the university employees (faculty and staff). We have had discussions with Information Technology Services (ITS) at the University of Memphis to cooperate and to provide support as needed. The contacts of our research partners and supporters include Tony Sharp (Director of Information Security, FedEx), Robert Jackson (CIO, University of Memphis), and Aaron Higbee (CTO, PhishMe).

We believe that this project will directly benefit our regional industry and community partners (e.g. FedEx and International Paper) by offering science-based insights regarding how to improve information security awareness and compliance in organizations. In addition, the outcomes of this research have great potential to be published in a top-tier research journal due to the significance of topic (security awareness and compliance is recognized as one of the most important issues in modern organizations) and the novelty of research approach (i.e., this project involves unique field data as well as collaborations with industry partners). Lastly, this research has the potential to lead to submissions for major grant funding initiatives given National Science Foundation's recognition of phishing and cyber security as an important research area.