Citation:

Xu, T., Singh, K., Rajivan, P. (Accepted). SpearSim: Design and Evaluation of Synthetic Task Environment for Studies on Spear Phishing Attacks. To appear In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*.

Link to pre-print paper:

http://students.washington.edu/tx29/paper/2021_HFES_SpearPhishingMethodsPaper.pdf

Abstract

Despite significant advancements in security technologies, phishing attacks continue to be rampant and successful because distinguishing phishing emails from real messages remains difficult to most end-users, mainly the targeted kinds known as spear-phishing. There is a severe lack of human factor studies on spear-phishing attacks due to lack of methods and datasets. We have designed a novel multi-player synthetic task environment, called SpearSim, for conducting laboratory experiments on spear-phishing attacks. Using SpearSim, we have conducted an experiment to understand how information exploitation in spear-phishing attacks influences end-user decision-making. This paper describes the SpearSim system's design and discusses the results from the experiment conducted with SpearSim. The experiment results show that people are more vulnerable to spear-phishing attacks when attackers can explore and exploit different kinds of personal information available to them about their targets. We discuss the implications of this research for the design of anti-phishing training solutions and privacy enhancing technologies.