Hook, Line and Sinker: Adversarial behaviors and strategies in phishing attacks

Prashanth Rajivan
Assistant Professor
Department of Industrial and Systems Engineering
University of Washington

Abstract: Phishing attacks are a cause of concern for everyone who rely on email communications. Phishing exploit cognitive weaknesses of people who are persuaded into performing insecure actions. One phishing email and one vulnerable person is all it takes for an attacker to succeed. Therefore, human factors research is necessary to understand the roots of deception in social engineering communications and how they may influence our decision making. In this talk, I will discuss experiments on dynamic decision making in the context of phishing. This talk will describe a new simulation paradigm developed for studying and modeling human behavior in phishing attacks from both the attacker and end-user perspectives in which the objective of the attacker is to increase error rate of end-user decision making through persuasion and deception. Finally, I will introduce follow-on research directions I am currently pursuing on spear-phishing and end-user phishing training.

Bio: Prashanth Rajivan is an assistant professor of Industrial and Systems Engineering and adjunct assistant professor of human centered design and engineering at the University of Washington. His research agenda is on the intersection of human factors and computer security. His areas of interests include security and privacy decision making, simulation and modeling, computer supported cooperative work, and applied cognitive science. Prior to this appointment, Prashanth Rajivan was a Postdoctoral Research Fellow at the Department of Social and Decision Sciences, Carnegie Mellon University, Pittsburgh. He holds a Ph.D. in Human Systems Engineering (2014) and M.S. in Computer Science (2011) from Arizona State University, USA. He is the author of several peer-reviewed publications and book chapters. His work on multi-agent models of teamwork in cyber defense was awarded the best student paper at HFES annual conference in 2014. His dissertation work was a finalist in the Human Factors Prize on Cyber Security in 2017.