INDUSTRIAL & SYSTEMS ENGINEERING
UNIVERSITY of WASHINGTON

TOWARDS AUTONOMOUS ANTI-PHISHING PROBING AND TRAINING DELIVERY

Dr. Prashanth Rajivan
Assistant Professor

ABSTRACT

Despite significant advancements in security technologies, phishing attacks continue to be rampant and successful because it is cognitively challenging for humans to distinguish phishing emails from real messages. One phishing email and one vulnerable person is all it takes for an attacker to succeed. To combat the rampant phishing and spear-phishing threats, companies primarily rely on manual and non-adaptive approaches to training human employees to detect attacks that algorithms miss. In this talk, I will discuss experiments we are conducting and models we are developing to understand dynamic decision making in the context of phishing. First, I will describe a new simulation paradigm we have developed for studying human behavior in phishing attacks from both the attacker and end-user perspective. Next, I will present results from a reinforcement learning model developed to predict and analyze human responses to phishing emails obtained from a laboratory experiment. I will describe the effectiveness of integrating natural language processing methods, such as, GloVe, and BERT with reinforcement learning models to predict human response to phishing emails. Finally, I will introduce follow-on research directions I am currently pursuing to develop adaptive and autonomous methods for effective anti-phishing training.

DATE/TIME

Nov. 22, 2022

1:30 pm - 2:20 pm PST

MEB 242

SPEAKER 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, simulation modeling and computer security. 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. 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. His research is funded by NSF, AHRQ, Starbucks and CISCO.