Dr. Ahmed Abbasi
University of Virginia

“The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites”

Abstract: User susceptibility to phishing websites is a significant security concern for organizations, both in terms of threats targeting employees and customer-facing attacks that undermine trust, satisfaction, and brand equity. At the root of the problem is the fact that users are ineffective at identifying and avoiding phishing websites. Even when using protective anti-phishing tools, many users remain vulnerable. In this study, we propose the Phishing Funnel Model (PFM), a robust design artifact for predicting user susceptibility to phishing websites. Leveraging the observe-orient-decide-act (OODA) loop for decision-making in risky, adversarial, real-time environments, PFM incorporates relevant user, threat, and tool-related factors to predict decisions and actions pertaining to four key stages of the phishing process: visit, browse, consider legitimate, and intention to transact. In order to estimate the model, we used a cumulative link mixed model for representing users’ decisions across funnel stages. We evaluated the susceptibility modeling potential of PFM relative to existing models in two extensive laboratory experiments involving 1,388 participants and nearly 7,000 observations. PFM was significantly better at predicting users’ phishing susceptibility behaviors, revealing that anti-phishing tool performance, tool perception, demographic, and prior experience-related variables were stronger indicators of users’ phishing susceptibility relative to threat characteristic constructs, suggesting that existing training and education programs’ emphasis on threat literacy might be misplaced. Furthermore, we tested the efficacy of PFM in a 12-month longitudinal field experiment at two organizations, involving 1,278 employees and 49,373 phishing interactions. PFM outperformed competing models in predicting employees’ susceptibility, providing strong external validity to our results. Our findings have important proactive implications for organizations’ anti-phishing strategies, including personalized real-time warnings, access controls, and data security policies that adapt over time.