EVALUATING PHISHING AWARENESS TRAINING PRODUCTS FOR REAL-WORLD ENTERPRISE USE

Steven McCarthy

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2023

Approved by

Advisory Committee

Dr. Jeffrey Cummings _____

Dr. Hosam Alamleh _____

_____
Dr. Geoff Stoker, Chair

Accepted By

_____
Dean, Graduate School

ABSTRACT

Evaluating Phishing Awareness Training Products For Real-World Enterprise Use. McCarthy, Steven, 2023. Capstone Paper, University of North Carolina Wilmington.

This paper discusses the evaluation, and eventual selection and implementation of a new phishing training platform, Cofense PhishMe, to improve reporting accuracy and enhance the overall security posture of an organization. The primary problem addressed in this capstone project was the difficulty in obtaining accurate data from the previous platform, Mimecast, due to multiple layers of defense and misconfiguration. The project evaluated two different phishing platforms and found that Cofense PhishMe provided more accurate reporting. The switch to the new platform also provided the ability to focus more on automation, reducing the time spent on tasks such as pulling and scanning bi-weekly threat submissions. The project was successful, with accurate reporting achieved during the phishing simulations, and the organization was able to improve its phishing training program and reduce the time spent creating the simulations and reporting. Lessons learned from the project include the importance of thoroughly understanding outcomes, building, and fully implementing new products, and the understanding the potential cost of implementing a project beyond the budget. This paper emphasizes the critical role of effective phishing training programs in educating employees on how to identify and respond to these threats and highlights the need for organizations to stay vigilant and proactive in protecting themselves against phishing attacks and using the best tools available to validate effectiveness.