

Name: Xavier Basnight

Date: March 30, 2025

Article Review #2: A Social Science Approach to Teaching Cybersecurity

Introduction

The article discusses how the inclusion of social science concepts in cybersecurity research can raise the level of awareness of social engineering attacks. It proposes a curriculum for different age groups with psychology, sociology, and anthropology to address the growing threat of cyber manipulation.

Social Science Principles and Research

The subject matter is directly applicable to social science by addressing how psychological and social vulnerabilities are being targeted during cyberattacks. It is addressing the human behavioral, trust, and cultural dynamics dimension of cybersecurity along with the fundamental principles of social science such as social influence and group behavior.

Relation between Course Ideas and Disenfranchised Populations

The research touches upon how a curriculum that is focused on social science can enhance the capability of people to detect and counter social engineering attacks. It predicts that integration of behavioral insights into education will create a security-aware culture. Secondary analysis of secondary literature and social engineering and education on cybersecurity case studies are utilized by the study. Effective practices such as gamification, scenario-based training, and ongoing learning programs are learned by the study. Qualitative case study data are utilized to evaluate the effect of educational practices by the study. Machine learning and behavioral analysis are also identified as personalization tools for training programs.

Contributions to Society

The article supports topic matter taught in PowerPoint courses on interdisciplinary methods with an emphasis on the ways in which social sciences help one understand human factors of cybersecurity. Principles such as behavioral analysis and cultural considerations form the core of the suggested curriculum. The article recognizes the need for adapting cybersecurity training to different populations, including children and oppressed groups. In trying to mitigate variation in digital security awareness through addressing variation in levels of access and awareness, it caters to diversity.

Conclusion

This research is a supplement to suggesting a novel method toward cyber attack resistance via education. It teaches individuals concrete skills along with gaining insight into societal vulnerabilities during the age of information. Finally, the integration of social science

fundamentals into cybersecurity training presents a more general solution to opposing social engineering attacks. By resisting human nature by technical defense measures, this strategy adds to overall societal resilience against next-generation cyber attacks.

Reference

1. **International Journal of Cybersecurity and Information Compliance.** (n.d.). *Bridgewater State University.* <https://vc.bridgew.edu/ijcic/>