Name: Mackenzi Dellolio

Date: March 31, 2025

Cybersecurity Behaviour and Measurement Instrument Development

This review discusses the development and evaluation of a cybersecurity behavior measurement tool for undergraduate students, examining its alignment with social science principles, its relevance to marginalized groups, and its potential to improve cybersecurity awareness and behaviors in society.

Introduction

The article “Development and Evaluation of a Cybersecurity Behaviour Measurement Instrument” details an extensive study to develop a robust, psychometrically sound measurement tool to measure cybersecurity behaviour, in this case focussed at undergraduate students. The work has strong implications in cyberspace behavior, providing a deeper understanding of belief-based measurement of cybersecurity, with the increasing threat of cybercrime and emphasis on proper measurement. This ties into the social sciences as it utilises principles of behavioural science to create an instrument designed to measure cybersecurity behaviours which can then be implemented to reduce behaviours and practices leading to insecurity.

Research Questions and Hypotheses

These primary research questions serve as the rationale for the validation of the cybersecurity behavior measurement tool. The authors tested the following hypotheses in their study:

1. Exploratory Factor Analysis (EFA) can effectively evaluate the cybersecurity behavior measurement instrument.

2. EFA can account for more than 60% of the variance in cybersecurity behavior.

3. Confirmatory Factor Analysis (CFA) will validate that the model satisfactorily fits the empirical data (Ngamcharoen, Sakdapat, & Bhanthumnavin, 2024).

Research Methods Used

The study used qualitative and quantitative research methods. Initially, the researchers utilized a literature review to define the variables and identify the components needed to assess cybersecurity behavior. The researchers then constructed a questionnaire based on the literature, which underwent expert review and pilot testing. Statistical analyses such as Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) were employed to evaluate the instrument's validity and reliability (Ngamcharoen et al., 2024). Additionally, an Independent-Sample t-test and Pearson's Correlation Coefficient analysis were used to assess the quality of individual items in the tool.

Types of Data and Analysis

The data collected included responses from a sample of 120 undergraduate students who were administered the cybersecurity behavior questionnaire. The responses were analyzed using two different statistical methods:

- EFA was conducted using Principal Component Analysis and Varimax Orthogonal Rotation, revealing that 21 items met the required criteria.

- CFA was used to confirm the validity of the measurement model, which indicated that the model fit the empirical data well (Ngamcharoen et al., 2024).

Marginalized Groups

The study primarily focuses on undergraduate students. This group is a highly engaged demographic in online activities, but may not always have strong cybersecurity practices. While the study does not directly focus on marginalized groups, the findings could have significant

implications for marginalized populations who are disproportionately affected by cyber threats, such as low-income communities and underrepresented racial or ethnic groups. By understanding students' behaviors, the research can help create interventions for vulnerable groups, making them better prepared for cybersecurity risks.

Connection to Social Science Principles

The topic of cybersecurity behavior measurement relates to several social science principles, especially in behavioral science and sociology. The study applies psychological theories to understand how individuals perceive and act upon cybersecurity threats. It also reflects on social learning theory, where the environment and social interactions influence behaviors (Ngamcharoen et al., 2024).

Overall Contributions of the Study to Society

The overall contribution of this study to society is multifaceted. It offers a validated tool for measuring cybersecurity behavior, which can be used in educational settings to raise awareness about cybersecurity threats. The tool could also inform policy development to improve cybersecurity education among students and the general public. Additionally, the study can influence educational curricula, public awareness campaigns, and cybersecurity training programs by providing insights into the behaviors that lead to more secure online practices.

Conclusion

In conclusion, the article provides valuable contributions to cybersecurity behavior measurement. It successfully develops and validates a comprehensive instrument to assess cybersecurity behaviors among undergraduate students. This research has significant implications for improving cybersecurity practices, particularly in educational institutions. The study's use of social science principles, such as behavioral science and psychology, highlights the importance of understanding human behavior in cybersecurity. Future research could adapt the tool for other populations, enhancing its societal impact.

References

Ngamcharoen, P., Sakdapat, N., & Bhanthumnavin, D. E. (2024). Development and evaluation of cybersecurity behaviour measurement instruments for undergraduate students. *International Journal of Cyber Criminology, 18*(1), 130–147. https://doi.org/10.5281/zenodo.4766807