Review of: "Maintaining cyberhygiene in the Internet of Things (IoT): An expert consensus study of requisite user behaviours"

J.I. Naser[1]

1 University of Tabriz

Potential competing interests: No potential competing interests to declare.

Introduction:

The introduction sets the stage well by defining the IoT and highlighting the security and privacy concerns associated with increased connectivity. It effectively emphasizes the need for cyberhygiene in IoT settings and the relevance of expert consensus in identifying key behaviors and threats. It would be helpful to provide a brief statement on the novelty or contribution of this study compared to existing research on IoT cybersecurity.

Method:

The method section provides a clear outline of the study design and participant selection process. The use of the Delphi method for gathering expert views and building consensus is appropriate for investigating complex issues like IoT security. However, it would be beneficial to briefly explain the Delphi method for readers unfamiliar with it. Additionally, while the demographic information of the participants is provided, it would be useful to mention the fields of expertise or industries represented by the participants to understand the diversity of perspectives.

Results:

The results section presents the outcomes of the Delphi rounds, including the consensus reached for protective behaviors, risk behaviors, and threats. The division of protective behaviors into lifecycle stages is a useful approach to enhance understanding and usability of the data. The consensus percentages for each category are well-presented, allowing readers to identify which behaviors achieved consensus and which areas require further discussion. It would be helpful to provide a summary of the top critical protective behaviors, risk behaviors, and threats based on the consensus scores.

Discussion:

The discussion is essential for contextualizing the findings and providing insights into the implications of the study. It should highlight the significance of the identified behaviors for improving IoT cybersecurity and potential applications in behavior change interventions. Consider addressing the limitations of the study, such as the potential biases associated with expert selection and the lack of representation from certain fields or regions.

Conclusion:

The conclusion should reiterate the key findings and their implications for maintaining cyberhygiene in the IoT. A succinct

summary of the critical behaviors and threats identified in the study could enhance the clarity of the conclusion.

Overall, this manuscript makes a valuable contribution to the understanding of requisite user behaviors for maintaining cybersecurity in the IoT. The study design and methodology are sound, and the results provide important insights for future research and practical applications. With some minor revisions, this manuscript will be suitable for publication in the target journal.