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

Arash Heidari[1]

1 Institute of Electrical and Electronics Engineers (IEEE)

Potential competing interests: No potential competing interests to declare.

Clarify the research objective: Begin the paper by clearly stating the objective of the study, which is to identify expert consensus on key protective behaviors, risk behaviors, and threats for IoT cybersecurity. This will provide a clear focus for the readers.

Provide more details on the Delphi consensus study: Elaborate on the methodology used in the Delphi consensus study, including the selection criteria for experts, the number of rounds conducted, and the rationale behind using this approach. This will help readers understand the rigor of the study.

Justify the use of the Delphi method: Discuss why the Delphi method was chosen as the appropriate approach for gathering expert consensus in this context. Highlight its advantages, such as anonymity, iterative feedback, and controlled feedback process.

Clearly define the behavioral categories: Provide explicit definitions and explanations of the behavioral categories derived from the experts' responses in Round One. This will enhance the clarity and consistency of the categorization process.

Provide a comprehensive list of the identified protective behaviors: Present a complete list of the 28 identified protective behaviors along with their definitions. This will enable readers to have a clear understanding of the specific behaviors that are considered crucial for IoT cybersecurity.

Include a detailed discussion of the risk behavior and threats: Provide an in-depth analysis and explanation of the identified risk behavior and six threats for IoT cybersecurity. Discuss the potential impact of these risk behaviors and threats on IoT breaches.

Compare and contrast with conventional computing settings: Conduct a thorough comparison between the identified protective behaviors for IoT and those for conventional computing settings. Highlight the similarities and differences, and discuss the rationale behind the overlap or variation in behaviors.

Discuss implications for behavior change interventions: Provide a comprehensive discussion on how the findings of the study can inform the development of tailored behavior change interventions to improve cybersecurity in IoT settings. Highlight the potential challenges and opportunities in promoting these behaviors.

Address limitations and future research directions: Acknowledge any limitations of the study, such as potential biases in expert selection or generalizability of findings. Additionally, suggest potential areas for future research, such as exploring the effectiveness of behavior change interventions based on the identified behaviors.

By incorporating these technical comments, the paper will provide a more comprehensive and insightful analysis of the expert consensus on protective behaviors, risk behaviors, and threats for IoT cybersecurity, thus enhancing its overall quality and impact.