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

Shokhan M. Al-Barzinji[1]

1 University of Anbar, Iraq

Potential competing interests: No potential competing interests to declare.

This paper effectively addresses the behavioral dimension of IoT cybersecurity, a critical yet underexplored area. However, its reliance on expert consensus without empirical validation limits its practical applicability. Greater detail on the methodology, findings, and implications would strengthen the study's contribution to the field. The abstract summarizes the objectives, methodology, and key findings of the study, which aimed to identify critical user behaviors for maintaining IoT cybersecurity.

Strengths:

1. Clearly outlines the purpose of the study: identifying protective behaviors, risk behaviors, and threats in IoT cybersecurity.
2. Describes the methodology (Delphi consensus study) effectively, giving credibility to the findings.
3. Highlights the importance of behavior adaptation in IoT contexts compared to conventional computing.
4. Lists specific protective behaviors, which ground the findings in actionable insights.

Furthermore, the paper would benefit from the inclusion of more updated references to strengthen its relevance and reliability. Integrating recent studies and findings related to the topic will demonstrate the author's awareness of current developments in the field and ensure that the paper remains up-to-date.

https://www.researchgate.net/publication/331049288_Internet_of_things_utilization_for_ehealthcare_monitoring

These enhancements will contribute to the overall quality and impact of the paper, enhancing its value to the academic community and readers interested in the subject matter.

Suggestions for Improvement

1. Include a brief description of the six threats identified.
2. Mention the number and diversity of experts to enhance credibility.
3. Add a clear distinction between IoT-specific and general cybersecurity risks.
4. Update cybercrime statistics to reflect current trends.
5. Provide actionable recommendations for key stakeholders, such as policymakers or device manufacturers.

6. Emphasize the importance of integrating cybersecurity education into IoT product design and marketing.