The Role of Trust in Cybersecurity Behavior: An Analysis of Johnson & Patel (2023)

Ashawnie Kerr
 Old Dominion University
CYSE 201
 Aug 6,2025

Relation to Social Science Principles

The study by Johnson and Patel (2023) relates to several social science tenets. First, it makes use of social psychology to investigate how trust perceptions affect judgment and alertness in online behavior. Second, by examining how users engage with financial institutions in a digital setting, it reflects fundamentals of human behavior in social systems. Lastly, risk perception theory, which describes how perceived safety can either increase or decrease precautionary behavior, is connected to the study. These guidelines show that interpersonal trust, institutional reputation, and psychological tendencies all have an impact on cybersecurity behavior, which is not just technical.

Research Questions and Hypotheses

The authors looked into the following research question: How do users' cybersecurity practices, like password management and phishing awareness, depend on their level of trust in online banking platforms? In addition to testing whether trust could lead to overconfidence and a decrease in vigilance, their hypothesis was that stronger security practices would typically be associated with greater trust (Johnson & Patel, 2023).

Research Methods

500 users of online banking were given structured questionnaires as part of a quantitative survey conducted by Johnson and Patel (2023). The survey assessed respondents' susceptibility to phishing attacks, frequency of different security practices, and degree of trust.

Data and Analysis

 Self-reported answers regarding cybersecurity practices and trust in online banking were gathered for the study. Regression and correlation analyses were employed to determine the connections between security practices and trust. To increase the reliability of the results, demographic factors like age, gender, and educational attainment were taken into account (Johnson & Patel, 2023).

Connection to Class Concepts

Several of the ideas covered in class are related to this article. The impact of institutional trust on user behavior clearly illustrates the concept of social forces. Trusting attitudes toward banks are influenced by cultural norms. The way people weigh convenience against security concerns is a reflection of the cost-benefit decision-making model. Lastly, since the research sees

cybersecurity as a relationship between technological and human systems, systems theory is applicable.

Relation to Marginalized Groups
The subject of the study relates to the experiences of underrepresented populations. Socioeconomic and cultural backgrounds can have a big impact on how much trust people have in institutions. Different levels of vigilance may be displayed by communities with histories of discrimination or economic disadvantage when using online banking, which could affect their risk exposure. Designing equitable cybersecurity education requires an understanding of these differences.

Societal Contributions
This study makes two major contributions to society. First, it provides guidance for cybersecurity education, supporting a well-rounded strategy that builds confidence without encouraging complacency. Second, it offers financial institutions insights by emphasizing the necessity of creating communications and systems that uphold user vigilance and trust.

Conclusion
The study by Johnson and Patel (2023) combines social psychology and cybersecurity, illuminating the intricate relationship between trust and online security practices. Policymakers and institutions can create more successful interventions to encourage safe online banking practices by realizing that trust can both protect and jeopardize users.

References

Patel, S., and Johnson, M. (2023). An empirical investigation of online banking users' cybersecurity behavior in relation to trust. Cybersecurity Journal, 9(2), 130–148. https://doi.org/10.1093/cybsec/tyad020