EJTAS ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Examining the Awareness of Mobile Money Users on Security Risks in Tanzania to Enhance Cybersecurity Literacy: A Case Study of Airtel Money

Dorothy William Nyamwihula
Department of Informatics, Institute of Accountancy Arusha, P.O. Box 2798, Arusha, Tanzania

Suggested Citation
Nyamwihula, D.W. (2024). Examining the Awareness of Mobile Money Users on Security Risks in Tanzania to Enhance Cybersecurity Literacy: A Case Study of Airtel Money. *European Journal of Theoretical and Applied Sciences, 2*(6), 536-543.
DOI: 10.59324/ejtas.2024.2(6).46

Abstract:

The proliferation of mobile money services in Tanzania has revolutionized financial inclusion, but it has also exposed users to increasing cyber threats. This study examines the level of cybersecurity awareness among mobile money users, focusing on Airtel as a case study, to identify gaps and opportunities for enhancing cybersecurity literacy. The research explores users' exposure to formal training, the impact of Airtel's educational materials, and users' confidence in securing their accounts. Findings reveal a significant lack of formal training, with most users relying on Airtel's security tips to develop cybersecurity knowledge. While these resources have improved user confidence, there is a demonstrated demand for structured workshops and comprehensive training programs. The study underscores the need for collaborative efforts between service providers, policymakers, and educational institutions to address these gaps. Enhancing cybersecurity literacy through accessible, interactive, and user-centred approaches is essential to fostering a secure mobile money ecosystem in Tanzania.

Keywords: *Mobile money, cybersecurity awareness, cybersecurity literacy, Airtel Tanzania, mobile money security, digital financial inclusion, user confidence, cybersecurity training.*

Introduction

Moses et al., (2023) noted that the rapid growth of mobile money services in Tanzania has transformed the financial landscape, providing millions of individuals with access to digital financial systems and fostering economic inclusion. However, as the adoption of these services expands, so also do the associated risks of cyber threats and fraud, which can undermine user confidence and compromise the security of financial transactions. Cybersecurity literacy has thus become a critical factor in safeguarding users and ensuring the continued growth and trust in mobile money platforms (Pallangyo, 2022).

This study focuses on examining mobile money users' awareness in Tanzania, with a specific emphasis on Airtel as a case study. As one of the leading mobile network providers in the country, Airtel has played a significant role in promoting financial inclusion through its mobile money services. However, the increasing sophistication of cyberattacks targeting mobile money users has highlighted the need for enhanced education and training to empower users to protect themselves effectively (Mkilia et al., 2023).

Cybersecurity awareness is not merely a technical issue but a socio-economic one, as low levels of literacy and limited access to information can exacerbate users' vulnerability to cyber threats. Understanding the current state of mobile money users' awareness is crucial for developing strategies that address these gaps and enhance overall cybersecurity resilience (Shalua and Semlambo, 2024). The role of service providers, such as Airtel, in disseminating information, offering training, and fostering a culture of proactive cybersecurity practices is central to this endeavour.

The study examines key areas of user awareness, including access to formal training, the effectiveness of educational materials provided by Airtel, and users' confidence in applying learned practices to secure their accounts. By exploring these dimensions, the research seeks to identify both the strengths and limitations of existing initiatives aimed at improving cybersecurity literacy among mobile money users in Tanzania. The findings of this research are expected to contribute to a deeper understanding of the challenges and opportunities in enhancing cybersecurity awareness. They will provide actionable insights for service providers, policymakers, and other stakeholders seeking to create a safer digital financial environment. Ultimately, the study underscores the critical need for collaborative and innovative approaches to equip mobile money users with the knowledge and tools necessary to navigate the complexities of the digital financial ecosystem securely.

Materials and Methods

The study is conducted in Airtel House in Dar es Salaam, Tanzania, focusing on the telecom industry's headquarters. The research philosophy is critical realism, which acknowledges the existence of an independent objective reality and the influence of social structures and power dynamics on our perception of reality. The study uses quantitative approach to examine complex social matters and identify prospects for societal transformation. The research design is a strategic blueprint that outlines the individuals involved, locations, and methods used to collect data. The study employs a quantitative method, using questionnaires to gather numerical information. This methodology achieves a more profound understanding of the phenomenon being studied. The target population for the research includes mobile money users registered with Airtel Company and employees at the Airtel Company headquarters. As of June 2023, Airtel had around 17.5 million subscribers using mobile money services, with 1.2 million of these subscribers based in Dar es Salaam. The study aims to provide a comprehensive understanding of the phenomenon being studied by examining the relationship between social structures and ideologies.

The study used the basic random sampling method to select a smaller subset from a larger population, allowing for generalizations about the wider population. The researchers used the lottery method, assigning a number to each individual in the datasets, to generate unbiased estimates of population characteristics. The research involved 156 respondents and used questionnaires, which were distributed on the Google platform. The Likert scale format was used to collect quantitative data, with ratings ranging from 1 to 5. The questionnaire was chosen for its expedited data acquisition and cost savings.

Data analysis was crucial for organizing and enhancing data, enabling comparisons, deriving significant insights, and formulating hypotheses. The study aimed to evaluate user knowledge of cybersecurity in mobile money usage using multiple regression analysis, which examines the level of correlation between a dependent variable and two or more independent variables. The researcher assessed the influence of each independent variable on the variability of the dependent variable.

Results

Quantitative Analysis

Objective 1: To explore the role of education and training in improving users' cybersecurity knowledge.

Table 1. Role of Education and Training in Improving Users' Cybersecurity Knowledge

Key: *1: Strongly disagree, 2: Disagree, 3: Neutral, 4: Agree, 5: Strongly agree*				
To explore the role of education and training in improving users' cybersecurity knowledge.	**N**	**Mean**	**Std.dev**	**Overall rating**
Have ever received any formal training or information on how to protect your mobile money account from fraud and cyber threats	138	1.84	.5784	Disagree
Airtel provides me with educational materials or security tips about mobile money safety	138	4.28	.5859	Agree
I would participate in workshops or training sessions on mobile money cybersecurity if they were offered by Airtel or other organization	138	4.84	.6173	Agree
I am confident in my ability to secure my mobile money account after receiving educational information from Airtel	138	4.23	.6205	Agree
My cybersecurity knowledge has increased since I purchased Airtel	138	4.67	.6592	Agree

Source: Researcher (2024)

The findings reveal significant insights into the role of education and training in enhancing users' cybersecurity knowledge, particularly in the context of mobile money safety. Each statement highlights users' experiences and perceptions regarding training, educational materials, and their subsequent confidence in managing cybersecurity risks associated with their mobile money accounts.

The first statement indicates that the majority of respondents have not received formal training or information on protecting their mobile money accounts from fraud and cyber threats, as evidenced by a mean score of 1.84, corresponding to a "Disagree" rating. This suggests a notable gap in structured cybersecurity education for users, which could be attributed to a lack of access to training programs or inadequate emphasis on user education by relevant stakeholders. The low standard deviation (.5784) implies consistency in responses, reinforcing the finding that formal training in this area is limited.

In contrast, the statement that Airtel provides educational materials or security tips about mobile money safety received a strong endorsement, with a mean score of 4.28 ("Agree"). This indicates that while formal training may be lacking, Airtel's efforts to disseminate educational materials are well-received and valued by users. The low standard deviation (.5859) underscores a shared perception among respondents that Airtel plays an active role in raising awareness about mobile money safety.

A strong willingness to participate in workshops or training sessions on mobile money cybersecurity is reflected in the third statement, which garnered the highest mean score of 4.84 ("Agree"). This finding highlights a significant demand for such initiatives among users. The high mean and consistent responses (.6173 standard deviation) suggest that users are highly

motivated to enhance their cybersecurity knowledge if given the opportunity. This presents an important opportunity for Airtel and other organizations to address the unmet educational needs of their customers.

The fourth statement shows that users feel more confident in securing their mobile money accounts after receiving educational information from Airtel, as indicated by a mean score of 4.23 ("Agree"). This suggests that the educational materials provided by Airtel are not only effective but also empower users to apply learned practices. The close alignment of responses (.6205 standard deviation) reflects a general consensus on the positive impact of these materials on users' confidence levels.

Lastly, the increase in cybersecurity knowledge since purchasing Airtel services received a mean score of 4.67 ("Agree"), which is both high and consistent (.6592 standard deviation). This finding indicates that Airtel's ongoing efforts to educate its customers are translating into tangible knowledge gains. The results suggest that users associate their improved understanding of cybersecurity directly with their engagement with Airtel.

Overall, these findings underscore the critical importance of education and training in improving users' cybersecurity knowledge, particularly in the domain of mobile money. While Airtel's provision of educational materials is commendable and has positively impacted users' confidence and knowledge, the lack of formal training remains a significant gap. There is a clear and expressed interest among users for more comprehensive workshops or training sessions, presenting a valuable opportunity for Airtel and other organizations to expand their educational initiatives. Bridging this gap can further empower users, enhance their cybersecurity resilience, and foster greater trust in mobile money services.

The data in Table 2 presents a correlation analysis examining the relationships between three key variables: *Users' Awareness*, *Education & Training*, and *Perceptions of Security*. The correlations are measured on a scale where values range from -1 to 1, with positive values indicating a direct relationship, negative values indicating an inverse relationship, and values closer to zero suggesting weak or no relationship. All correlations marked with an asterisk (*) are significant at the 0.05 level, indicating a less than 5% probability that these results occurred by chance.

The self-correlation of each variable with itself is, as expected, 1.00, reflecting perfect correlation. The analysis highlights the following significant relationships:

1. **Users' Awareness and Education & Training**: The correlation coefficient of 0.56 indicates a moderate positive relationship between users' awareness, education, and training. This suggests that as education and training opportunities increase, users' awareness of cybersecurity also tends to improve. It emphasizes the role of structured learning initiatives in enhancing awareness.

2. **Users' Awareness and Perceptions of Security**: The correlation coefficient of 0.63 demonstrates a stronger positive relationship between users' awareness and their perceptions of security. This indicates that higher levels of awareness are associated with improved perceptions of personal and account security, reflecting the importance of knowledge in shaping users' confidence and attitudes toward cybersecurity practices.

3. **Education & Training and Perceptions of Security**: The correlation coefficient of 0.48 indicates a moderate positive relationship between education and training and perceptions of security. While the relationship is somewhat weaker than that of awareness and perceptions of security, it still underscores the contribution of educational initiatives in fostering a sense of security among users.

In summary, the data demonstrates significant interrelationships between the three variables, highlighting the interconnected roles of education and training, awareness, and perceptions of security. Education and training serve as a foundational element that positively influences both awareness and security perceptions, while awareness itself strongly correlates with users' sense of security. These

findings reinforce the critical need for targeted educational efforts to build a secure and confident user base in mobile money ecosystems.

Table 2. Correlation Analysis

Variable	Users' Awareness	Education & Training	Perceptions of Security
Users' Awareness	1.00	0.56*	0.63*
Education & Training	0.56*	1.00	0.48*
Perceptions of Security	0.63*	0.48*	1.00

Note: *Correlation is significant at the 0.05 level (2-tailed).

Discussion

The results present an insightful overview of how education and training influence users' cybersecurity knowledge in the context of mobile money. They reveal a complex interplay between the availability of formal training, the dissemination of educational materials, users' confidence in applying what they learn, and their motivation to further enhance their knowledge through workshops or training sessions.

A significant gap is evident in the provision of formal training for users on securing mobile money accounts from cyber threats. This deficiency underscores a systemic issue in cybersecurity education, where formal, structured programs remain largely inaccessible or underprioritized for end-users. The data indicates a uniform experience among respondents, suggesting a widespread lack of institutionalized training efforts. This limitation highlights an urgent need for collaborative initiatives between service providers, government agencies, and educational institutions to design and deliver comprehensive training programs tailored to users' needs.

Despite the absence of formal training, Airtel plays a proactive role in disseminating educational materials and security tips. This approach bridges gaps in user awareness and equips customers with practical knowledge about safeguarding their accounts. The success of these materials lies in their ability to convey critical security information in an accessible and digestible format, as reflected in the high agreement levels among respondents. However, while these resources are valuable, they cannot substitute the depth and interactivity of formal training, particularly for addressing nuanced or evolving cybersecurity threats.

The strong willingness of users to participate in workshops or training sessions is particularly noteworthy. It signifies a latent demand for deeper engagement and learning opportunities beyond the current offerings. This enthusiasm presents an excellent opportunity for service providers and other stakeholders to organize targeted training programs. Workshops can serve as an interactive platform for addressing users' specific concerns, debunking myths, and fostering a culture of proactive security practices. By tapping into this readiness, stakeholders can significantly enhance the cybersecurity landscape, both for individual users and the broader ecosystem.

Confidence in managing mobile money security is another crucial aspect that emerges from the findings. Users report feeling empowered after engaging with Airtel's educational resources. This confidence is an encouraging sign of the practical impact these materials have on behaviour and decision-making. However, confidence alone is not sufficient unless accompanied by robust and sustained learning experiences. Overconfidence without a solid foundation of comprehensive knowledge can sometimes lead to complacency, making it imperative to supplement educational efforts with more rigorous training and regular updates.

Finally, the reported increase in cybersecurity knowledge since purchasing Airtel services underscores the cumulative impact of consistent, user-centric educational initiatives. This progress

reflects Airtel's commitment to promoting cybersecurity awareness, a critical factor in building trust and loyalty among its customer bases. Nevertheless, sustaining this upward trajectory will require ongoing innovation and responsiveness to emerging cybersecurity challenges. Regular updates to educational content, incorporating feedback from users, and leveraging advanced tools such as gamification or simulation-based training can help maintain and enhance user engagement.

In summary, the results highlight the pivotal role that education and training play in equipping users with the skills and confidence to manage cybersecurity risks effectively. While Airtel has made commendable strides in providing accessible and impactful educational resources, there remains a pressing need for formal training programs to fill existing gaps. Harnessing users' demonstrated interest in learning and expanding these efforts through collaborative, innovative approaches will be crucial in fostering a secure and resilient mobile money ecosystem.

Conclusion

The research highlights the critical role of education and training in enhancing users' cybersecurity knowledge, particularly in the context of mobile money services. The findings reveal a dichotomy between the availability of formal training and the effectiveness of informal educational initiatives, emphasizing both the strengths and limitations of existing efforts to empower users in safeguarding their mobile money accounts.

It is evident that the lack of formal training has created a significant gap in users' ability to address complex and evolving cyber threats. However, Airtel's provision of security tips and educational materials has emerged as a key driver of increased awareness and confidence among users. These resources, while impactful, underline the necessity for more comprehensive and structured approaches to cybersecurity education. The demonstrated willingness of users to participate in workshops or training sessions underscores the untapped potential of interactive and immersive learning opportunities, which could significantly enhance their practical skills and preparedness.

The research also illustrates a strong correlation between the accessibility of educational initiatives and users' confidence in applying cybersecurity practices. This relationship suggests that sustained efforts to educate users—through a combination of formal training, tailored resources, and interactive platforms—can foster a culture of proactive and informed behaviour, mitigating risks associated with mobile money fraud and cyber threats.

In conclusion, the study underscores the urgent need for collaborative efforts among service providers, policymakers, and educational institutions to address the deficiencies in formal training while expanding the reach and depth of informal educational programs. By leveraging the evident demand for learning and building on existing initiatives, stakeholders can create a more secure digital environment for mobile money users. The findings serve as a call to action for developing holistic strategies that integrate education, innovation, and user engagement to fortify cybersecurity awareness and resilience.

Recommendations

Based on the findings, it is recommended that a multifaceted approach be adopted to improve users' cybersecurity knowledge and practices in the context of mobile money services. Service providers, such as Airtel, should consider complementing their existing educational initiatives with formal, structured training programs. These programs should be designed to address diverse user needs and levels of understanding, ensuring accessibility for all demographics, including those in underserved or rural areas. Workshops and training sessions, tailored to the specific challenges and risks faced by users, should be prioritized to provide hands-on learning experiences that go beyond basic information dissemination.

Additionally, collaboration between service providers, government agencies, and educational

institutions is essential to establish a unified and comprehensive framework for cybersecurity education. Policymakers should work with industry stakeholders to develop standardized training curricula and certifications that align with the evolving nature of cyber threats. These efforts should also include the integration of cybersecurity awareness into broader digital literacy initiatives, recognizing that financial and technological inclusion must be accompanied by adequate protective knowledge.

Furthermore, service providers should continuously update and innovate their educational materials to reflect emerging threats and best practices. Leveraging modern technology, such as interactive online platforms, gamification, and simulation-based learning, can enhance engagement and retention of information among users. Regularly soliciting feedback from users can also ensure that educational content remains relevant and user centric.

To sustain and amplify the positive impact of education on user confidence and behaviour, it is also recommended that Airtel and similar organizations adopt a continuous learning approach. This can include periodic refresher courses, updates through mobile alerts, and real-time guidance via customer support channels. Offering incentives for participation in training sessions, such as discounts or rewards, can further encourage user engagement and foster an initiative-taking approach to cybersecurity.

Acknowledgement

I begin by expressing my deepest gratitude to God for His guidance, strength, and unwavering grace that have sustained me throughout this journey.

I am profoundly grateful to my research supervisor for their invaluable expertise, constructive feedback, and unwavering support. Your mentorship has been a cornerstone in shaping this study and has inspired me to strive for excellence.

To my beloved family, I owe an immeasurable debt of gratitude. Your constant encouragement, patience, and unconditional love have been my greatest source of strength and motivation. You have been my refuge in moments of doubt and my cheerleaders in times of progress. Your sacrifices, understanding, and belief in me have not only fueled my determination but have also reminded me of the importance of perseverance and faith.

I also extend my heartfelt thanks to Airtel Tanzania for providing the resources and support essential for conducting this research.

To the participants of this study, I am deeply indebted to you for your willingness to share your insights and experiences, which have formed the backbone of this work.

Finally, to all who contributed in any way to this research, I extend my sincerest gratitude. Your support and encouragement have been instrumental in bringing this study to fruition.

Conflict of Interests

No conflict of interest.

References

Juma, Y. H. (2022). Assessing the Mobile Money user's awareness on social engineering in Tanzania: Case of the Ministry of Information Tourism and Heritage Zanzibar. *International Journal of Novel Research in Engineering and Science*, *9*, 27-34.

Lashitew, A. A., van Tulder, R., & Liasse, Y. (2019). Mobile phones for financial inclusion: What explain the diffusion of mobile money innovations? *Research Policy*, *48*(5), 1201–1215. https://doi.org/10.1016/j.respol.2018.12.010

Malero, A., & University of Dodoma. (2015). Measuring security awareness on mobile money users in Tanzania. *International Journal of Engineering Trends and Technology*, *20*(1), 44–47. https://doi.org/10.14445/22315381/ijett-v20p210

Mkilia, E., Kaleshu, J. T., & Sife, A. S. (2023). Cybersecurity risks and customers' Protective

Behaviour on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania, 329.

Moses, N., Semlambo, A. A., & Sabaya, D. P. (2023). The Impacts of Cybercrime on the Growth of Mobile Money Services in Tanzania; A Case of Kongwa District. *GPH-International Journal of Business Management*, *6*(11), 42-63.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. *Predicting and changing health behaviour: Research and practice with social cognition models*, *3*, 70-106.

Pallangyo, H. J. (2022). Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. *Tanzania Journal of Engineering and Technology*, *41*(2).

Shalua, N. S., & Semlambo, A. A. (2024). Strengthening Tanzania's Digital Infrastructure: Assessing Cyber Threats to the Government e-Payment Gateway for National Security. *Educational Research (IJMCER)*, *6*(4), 192-205.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150