**Evaluating Cybersecurity Awareness Levels among NMB Bank Plc. Customers in Morogoro Municipality**

**ABSTRACT**

This study evaluates the level of cybersecurity awareness among customers of NMB Bank Plc in Morogoro Municipality, Tanzania, in the context of the increasing adoption of digital banking services. The rapid digitalisation of banking platforms has created new opportunities for financial inclusion, while simultaneously exposing users to heightened risks such as phishing, identity theft, and online fraud. Despite significant investments in digital infrastructure, limited cybersecurity literacy remains a major vulnerability within Tanzania’s banking ecosystem. The study employed a cross-sectional design within a mixed-methods framework, combining quantitative data from 375 customer questionnaires with qualitative insights from ICT champions at selected NMB branches. The findings revealed a high level of general awareness, particularly regarding the risks of sharing personal banking information (88.5% agreement; M = 4.27, SD = 0.85; χ² = 579.59, *p* < 0.001) and understanding the impact of cyber fraud (81.6% agreement; M = 4.10, SD = 0.89; χ² = 411.48, *p* < 0.001). However, practical knowledge and behavioural skills were limited. Only 39% of customers had attended cybersecurity training (M = 2.98, SD = 1.33; χ² = 7.15, *p* = 0.051), and just 47% could identify signs of a hacked account (M = 3.33, SD = 1.22; χ² = 25.12, *p* = 0.015). These results indicate a significant gap between theoretical awareness and applied cybersecurity practices. The study concludes that while awareness of cybersecurity threats is relatively high, gaps in practical training and situational readiness persist, increasing vulnerability among digital banking users. Policy implications include integrating cybersecurity education into national financial literacy programmes, mandating customer-centred awareness initiatives by financial institutions, and establishing a national cyber hygiene policy. Strengthening end-user awareness is critical to enhancing the resilience and security of Tanzania’s digital financial system.

**Keywords:** *Cybersecurity awareness, digital banking security, financial literacy, customer behaviour, Tanzania, NMB Bank Plc.*

1. **Introduction**

The global shift towards digital financial services has transformed the banking sector, making it more accessible, efficient, and customer-centred. Thus, innovations such as mobile banking, online payments, and electronic transfers have become integral to everyday banking experiences. In Tanzania, as in many other developing nations, this digital transformation has seen widespread adoption across both urban and rural populations, largely due to the increased penetration of smartphones and improved mobile network coverage (Wang, 2024). However, the parallel rise in cyber threats has posed significant challenges to this transformation. Cybersecurity, the practice of protecting digital systems, networks, and user data from cyberattacks, is increasingly crucial in the banking sector. As customers embrace digital banking platforms, they are exposed to various forms of cybercrime, including phishing scams, malware infections, identity theft, and data breaches. Globally, nearly 70% of financial institutions have reported experiencing cyberattacks, while over 40% of internet users have been victims of cybercrime (Zwilling, 2020). These statistics reflect an urgent need for improved cybersecurity awareness, especially among banking customers who may lack adequate knowledge or digital safety skills.

In Africa, and more specifically in sub-Saharan Africa, the situation is particularly alarming. The rapid growth of digital financial services has not been matched by a corresponding increase in cybersecurity literacy among users. Institutions such as the African Union Commission have expressed growing concern over the frequency of mobile money fraud and internet banking scams. Countries like South Africa, Kenya, and Nigeria have experienced a marked increase in cyber-related crimes, largely attributable to users’ limited awareness of online safety practices (Wamala *et al*., 2020).

Within the East Africa region, mobile financial services such as M-Pesa have significantly enhanced financial inclusion by providing access to the unbanked (United Republic of Tanzania [URT], 2017). Nevertheless, they have also introduced new security vulnerabilities. Studies in Kenya and Uganda reveal that many digital banking users do not regularly update their passwords, use insecure internet connections, and are unaware of key protective features such as two-factor authentication (Wamala *et al*., 2020). This lack of awareness makes users vulnerable to cybercriminals and undermines the security infrastructure put in place by financial institutions.

In Tanzania, the growth of digital banking is most visible in urban areas like Morogoro Municipality, where banks such as National Microfinance Bank (NMB) Plc have expanded mobile and internet-based services. Nevertheless, alongside this growth is an uptick in cyber threats including ransomware, phishing, and financial fraud (NMB, 2020a). NMB Bank Plc, one of the leading financial institutions in Tanzania, has invested in digital infrastructure to enhance customer experience and service delivery. Yet, as digital usage increases, the gap in customer cybersecurity awareness becomes more evident. Customers frequently fail to identify fraudulent websites, respond appropriately to suspicious emails, or implement basic safety protocols like password management (NMB, 2020b). Despite efforts by financial institutions and government agencies to address cybersecurity threats, there remains a lack of comprehensive public education on digital safety. Inadequate awareness creates a weak link in the cybersecurity chain, as uninformed users often unintentionally expose themselves and their financial institutions to cyber threats. According to Wang (2024), many Tanzanian users lack even the most basic knowledge about the risks of using public Wi-Fi for banking transactions. Without enhanced awareness, customers are not only at risk themselves but may also compromise the security of the broader banking ecosystem. Further evidence from Shulha *et al*. (2022) underscores the importance of contextualising cybersecurity education within local realities. In Tanzania, many cybersecurity campaigns are limited in reach and content, failing to effectively engage bank clients, particularly those who are not technologically savvy. Moreover, the lack of integration between cybersecurity training and financial literacy programmes limits their overall impact.

Given these realities, there is a need to assess the current state of cybersecurity awareness among bank customers, especially those utilising digital banking services. Morogoro Municipality provides a fitting context due to its increasing urbanisation and growing adoption of online banking services. This study focuses specifically on NMB Bank Plc customers in this municipality, aiming to determine their awareness levels, evaluate their behavioural practices, and identify knowledge gaps. As such, understanding how customers perceive cyber threats and what protective measures they undertake is vital for financial institutions striving to provide secure services. This study, therefore, contributes to this endeavour by exploring the extent to which NMB Bank Plc customers in Morogoro Municipality are equipped to deal with the risks associated with digital banking. It fills an important gap in the literature by focusing on the end-user’s awareness and behaviour, which are often overlooked in institutional and technical cybersecurity assessments. The findings will be essential not only for NMB Bank Plc but also for other financial institutions and policymakers seeking to enhance cybersecurity resilience in Tanzania’s digital economy.

1. **Theoretical perspective**

This study was guided by the Protection Motivation Theory (PMT), a behavioural theory developed by Rogers (1975) to explain how individuals are motivated to adopt protective behaviours when confronted with perceived threats. The theory has since been widely applied in the fields of health psychology (Milne *et al*., 2006), environmental behaviour, and, more recently, information security and cybersecurity awareness. PMT is particularly relevant for evaluating how individuals respond to cyber risks and what motivates them to adopt safe online practices. Its applicability to this study lies in its focus on both the perception of threats and the perceived ability to cope with those threats, elements central to understanding cybersecurity awareness among bank customers. The theory is grounded on two major cognitive processes: *threat appraisal* and *coping appraisal*. Threat appraisal assesses how customers evaluate the potential harm associated with a threat and their vulnerability to it. In the context of this study, it relates to how NMB Bank Plc customers perceive the severity of cyber threats, such as phishing, identity theft, and online fraud, and the likelihood that they themselves might fall victim. Customers who perceive high severity and vulnerability are more likely to be motivated to take action to protect themselves. For instance, awareness of the consequences of clicking on malicious links or using insecure Wi-Fi connections can influence whether individuals take precautions while using digital banking platforms.

Coping appraisal, on the other hand, refers to how individuals assess their ability to manage or avoid the threat. This includes response efficacy, the belief that certain protective measures (like two-factor authentication or regular password updates) are effective, and self-efficacy, which reflects an individual’s confidence in their ability to perform these protective actions. In this study, coping appraisal was essential in understanding whether customers believed that their actions could make a difference in protecting their personal and financial information and whether they felt competent enough to carry out those actions. Thus, using PMT as a guiding framework, the study was able to structure its investigation into the awareness, perceptions, and behaviours of customers in relation to cybersecurity. Survey questions were designed to explore customers’ knowledge of cyber threats (threat appraisal), their trust in protective mechanisms, and their confidence in applying them (coping appraisal). This helped in assessing the depth of cybersecurity awareness among different demographic groups and in identifying behavioural patterns that could inform targeted awareness campaigns.

1. **Materials and methods**

**3.1 Study area**

The study was conducted in Morogoro Municipality, focusing specifically on branches of National Microfinance Bank (NMB) Plc. NMB Bank Plc was chosen due to its extensive customer base and leading role in delivering digital financial services in Tanzania (NMB, 2024). According to 2024 NMB annual report, the shift toward digital banking continued to accelerate, with 96% of retail transactions now conducted through alternative channels (NMB, 2024). Morogoro Municipality, with its growing urban population and increased uptake of digital financial platforms, provided a relevant and dynamic setting for investigating cybersecurity awareness. The area is characterised by a mix of individual and institutional banking customers, thus offering a diverse respondent base for the study

**3.2 Research design and approach**

This study adopted a cross-sectional research design within a mixed-methods approach to evaluate cybersecurity awareness among customers of NMB Bank Plc in Morogoro Municipality. The cross-sectional design enabled the collection of data at a single point in time, allowing the researchers to capture a snapshot of customers’ awareness levels, behaviours, and perceptions related to cybersecurity in the context of digital banking (Creswell, 2014). This design was particularly suitable for identifying prevailing trends and patterns without manipulating the study environment. To enhance the depth and breadth of the investigation, a mixed-methods approach was employed, integrating both quantitative and qualitative techniques. The quantitative component facilitated the systematic collection and statistical analysis of numerical data to assess the level of awareness and behavioural patterns among banking customers (Creswell, 2014). In contrast, the qualitative component offered deeper insights into participants’ personal experiences, perceptions, and attitudes regarding cybersecurity, particularly those aspects that are often difficult to quantify (Bryman, 2016).

**3.3 Target population**

The study targeted two main groups: NMB Bank Plc customers and branch ICT champions. Customers were selected as the primary focus of the study because they are the end-users of digital banking platforms and therefore directly impacted by cybersecurity threats. Their awareness levels and behavioural practices play a critical role in maintaining digital security. The inclusion of ICT champions, staff members responsible for the implementation and oversight of information and communication technology within the bank, was intended to provide an institutional perspective on cybersecurity strategies and operational challenges. Their expert insights were valuable in contextualising the findings from customer responses.

**3.4 Sample size and sampling procedures**

The sample size for customer respondents was determined using Cochran’s (1977) formula, which is appropriate for large populations when the population proportion is unknown. The formula is expressed as:

$n=\frac{Z^{2} . p . q}{e^{2}}$ (1)

where:

$n =$ required sample size

$z = $Z-value for a 95% confidence level (1.96)

$p =0.50 $ (estimated proportion of the population with the attribute in question).

$e =0.05 $ margin of error (0.05)

$q = 1 – p$ (2)

Combining Equation (1) and (2), the Cochran (1977) formula becomes:

$n=\frac{z^{2} . p . (1-p)}{e^{2}}$ (3)

Substituting the values into the formula:

$n=\frac{(1.96)^{2}×0.50×(1-0.50)}{(0.05)^{2}}$ (4)

$n=384.16$ (5)

Thus, the sample size was rounded up to 385 customer respondents. As for the ICT champions, a census sampling technique was adopted. Given the limited number, only five individuals at the selected NMB Bank Plc branches, all were included in the study to ensure comprehensive coverage and to capture expert institutional perspectives on cybersecurity practices. With regard to NMB customer selection, the study employed a convenience sampling technique. This non-probability method enabled the researchers to approach readily available and willing participants, facilitating efficient data collection under time and logistical constraints. Nonetheless, it is acknowledged that convenience sampling may introduce some level of selection bias, potentially affecting the generalisability of the findings. Despite this, the combined use of census and convenience sampling provided a practical and inclusive basis for obtaining both customer-level and institutional-level insights into cybersecurity awareness.

**3.5 Data types, sources and collection methods**

This study utilised both primary and secondary data to provide a comprehensive assessment of cybersecurity awareness among NMB Bank Plc customers in Morogoro Municipality. The primary data comprised first-hand information collected directly from two categories of respondents: (i) customers of NMB Bank Plc, and (ii) branch ICT champions. These data captured participants' knowledge, perceptions, attitudes, and practices related to cybersecurity and digital banking. The secondary data included relevant literature, policy documents, institutional reports, and previous research studies on cybersecurity awareness, particularly in the context of developing countries and digital financial services. These sources helped to contextualise the study findings and strengthen the theoretical grounding.

We used structured questionnaires which were administered to NMB Bank Plc customers. The questionnaires included closed-ended questions and Likert-scale items designed to assess the respondents’ understanding of cybersecurity risks, frequency of secure online behaviours, and their use of protective features such as strong passwords and two-factor authentication. This method facilitated the collection of quantifiable data for statistical analysis. Moreover, we used semi-structured interviews for ICT champions to collect qualitative insights into the bank’s internal cybersecurity policies, customer engagement practices, and institutional challenges in promoting digital safety. The semi-structured format allowed for flexibility in probing deeper into key issues while maintaining a consistent thematic focus.

**3.6 Data analysis**

Prior to data analysis, collected primary data underwent cleaning and validation, which involved screening the returned questionnaires for completeness and consistency. Using the Statistical Package for the Social Sciences (SPSS) Version 25, we performed a descriptive analysis to generate frequencies, percentages, means, and standard deviations, to assess the overall level of cybersecurity awareness among customers. These descriptive measures provided insights into patterns of agreement, indecision, and disagreement with specific cybersecurity statements. To assess the internal consistency and distribution of responses for each cybersecurity awareness statement, mean scores and standard deviations were calculated. Higher mean scores indicated stronger agreement and, by implication, higher awareness levels, whereas lower mean values suggested limited awareness or uncertainty. Furthermore, the chi-square (χ²) test of independence was used to determine whether the distribution of responses differed significantly from a uniform distribution across the Likert scale categories. A significance level of *p* < 0.05 was adopted as the threshold for statistical inference. This test allowed the researchers to assess whether the observed response patterns were statistically significant and not due to chance.

1. **Results and discussions**

**4.1 Response rate**

Of the 385 questionnaires distributed to customers within the study area, 375 were fully completed and returned, yielding a high response rate of 97.4%. The remaining 10 questionnaires (2.6%) were excluded from analysis due to substantial missing data, in accordance with established methodological standards (Schutt, 2019; Msambali & Mwonge, 2025). This exceptionally high response rate enhances the statistical validity of the study by reducing the likelihood of nonresponse bias, a common limitation in survey-based research. As such, the data derived from the 375 valid responses are considered both reliable and representative of the broader customer population under investigation (Mwonge & Naho, 2024). Moreover, the strong level of participant engagement suggests a high degree of relevance and resonance of the research topic among respondents, thereby reinforcing the robustness and credibility of the empirical findings.

**4.2 Cybersecurity awareness among NMB customers**

In this study, researchers sought to understand cybersecurity awareness among NMB Bank Plc customers in Morogoro Municipality due to the rising risks associated with digital banking services, such as phishing, identity theft, and online fraud. As customers increasingly rely on mobile and internet banking, their level of awareness becomes critical in safeguarding both their personal financial information and the integrity of the banking system (NMB, 2024). Despite the rapid adoption of digital platforms, there remains a significant gap in cybersecurity education and preparedness, particularly in developing regions like Tanzania. Table 1 presents the study results.

**Table 1: Customer responses on cybersecurity awareness (n = 375)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Cybersecurity awareness statement | DisagreeF (%) | UndecidedF (%) | AgreeF (%) | Mean | SD | Chi-square (χ² ) | p-value |
| I understand cybersecurity in online banking | 30 (8.0) | 60 (16.0) | 285 (76.0) | 3.98 | 0.97 | 328.27 | 0.000 |
| I can identify signs of a hacked bank account | 87 (23.2) | 112 (29.9) | 176 (47.0) | 3.33 | 1.22 | 25.12 | 0.015 |
| I have attended cybersecurity training | 152 (40.5) | 77 (20.5) | 146 (39.0) | 2.98 | 1.33 | 7.15 | 0.051 |
| I feel confident in identifying cyber threats | 56 (14.9) | 76 (20.3) | 243 (64.8) | 3.73 | 1.04 | 148.63 | 0.000 |
| I understand the impact of cyber fraud | 32 (8.5) | 37 (9.9) | 306 (81.6) | 4.10 | 0.89 | 411.48 | 0.000 |
| I protect my mobile banking applications | 53 (14.1) | 57 (15.2) | 265 (70.7) | 3.81 | 1.09 | 251.87 | 0.000 |
| I am aware of the risks of sharing personal banking information | 23 (6.1) | 20 (5.3) | 332 (88.5) | 4.27 | 0.85 | 579.59 | 0.000 |

***Source:*** Field data, 2024

The study results in Table 1 present a statistical summary of the responses from 375 NMB Bank Plc. customers with regard to their cybersecurity awareness. The results reveal varying levels of knowledge and confidence across key cybersecurity domains, with significant implications for customer safety and institutional risk management.

The highest levels of awareness were observed in customers' understanding of the risks associated with sharing personal banking information, where 88.5% agreed, yielding a very high mean score (M = 4.27, SD = 0.85) and a highly significant chi-square result (χ² = 579.59, *p* < 0.001). This suggests that customers are highly aware that disclosing sensitive information can expose them to fraud. The study results align with those by Shukla *et al*. (2025), Zwilling *et al*. (2020) and Suh *et al*. (2017) who collectively demonstrated data privacy as a well-recognised concern among digital banking users.

Similarly, understanding the impact of cyber fraud (M = 4.10, SD = 0.89) and protection of mobile banking applications (M = 3.81, SD = 1.09) also showed strong awareness, with 81.6% and 70.7% of respondents respectively, acknowledging the importance of these issues. These results align with findings by Choudhuri *et al*., (2024), who contend that mobile banking users often understand the general importance of security but may not always apply best practices effectively. This is further supported by Wamala *et al*. (2020), who notes that while knowledge of threats may exist, behaviour does not always align with risk prevention measures.

Conversely, areas of practical skills and behavioural training reflected weaker awareness. Only 39% of participants had attended any form of cybersecurity training, with a relatively low mean score (M = 2.98, SD = 1.33) and marginal significance (χ² = 7.15, *p* = 0.051). This is concerning, as training has been shown to significantly improve users' ability to identify and respond to cyber threats (Zwilling *et al*., 2020; Shaw *et al*., 2009; Dodge *et al*., 2007). Interviews conducted with ICT champions revealed that such training is not routinely offered to clients, which contributes to the observed gaps.

Likewise, recognition of signs of a hacked bank account yielded a mixed result, with 47% agreeing they could identify such signs, but nearly 30% remained undecided, and 23% disagreed. The mean score was a moderate 3.33 (SD = 1.22), indicating uncertainty in detecting actual breaches. This gap highlights the limitations in customers' situational awareness, an area that Choudhuri *et al*., (2024) reported as a major vulnerability in user-level cybersecurity. Another key result was customers' confidence in identifying cyber threats (64.8% agreement, M = 3.73, SD = 1.04), showing that while theoretical knowledge exists, confidence in applying that knowledge is still moderate. This finding corresponds with Creswell (2014), who states that the absence of experiential learning can limit individuals' ability to act effectively in real-world security contexts.

Overall, the results suggest a bifurcation in awareness: while general knowledge on digital security concepts is relatively strong, customers lack training-based, applied understanding. This division creates a weak link in the banking cybersecurity chain, as customers unaware of operational threats may inadvertently undermine institutional protections. As discussed by Shulha *et al*. (2022), improving customer literacy through continuous, localised awareness programmes is essential for building digital resilience, especially in developing economies like Tanzania.

1. **Policy and practical implications**

The findings of this study carry important implications for both policy formulation and institutional practice in the domain of cybersecurity and digital financial services. Firstly, there is an urgent need to integrate cybersecurity education into national financial literacy programmes. Given the observed knowledge gaps, particularly in practical skills such as recognising cyber threats and responding appropriately, policymakers, including the Bank of Tanzania and the Ministry of Finance and Planning, should ensure that digital safety training becomes a mandatory component of financial inclusion strategies. Embedding cybersecurity awareness into national frameworks will support the development of a digitally resilient banking population.

In addition, regulatory bodies should require financial institutions to implement structured and continuous cybersecurity awareness campaigns. These campaigns should be localised, multilingual, and accessible to diverse customer groups, including the digitally marginalised. A national cyber hygiene policy for end-users should also be established to promote safe digital behaviour and to set minimum awareness benchmarks for those utilising digital financial services. This policy should be supported by regular evaluations of cybersecurity practices by service providers.

Practically, financial institutions such as NMB Bank Plc must assume a more proactive role in educating their clients. The low proportion of respondents who have attended any form of cybersecurity training points to a critical need for structured, customer-centred educational initiatives. Banks should consider deploying digital literacy ambassadors at branch and community levels to facilitate ongoing awareness sessions. These ambassadors would be particularly effective in engaging customers who lack digital literacy, such as elderly users or those in peri-urban areas.

Moreover, there is a need to enhance the design of banking applications and interfaces to make security features such as two-factor authentication and password protection more user-friendly. Simplifying these processes will encourage greater usage and adherence to safe online practices. Banks should also introduce responsive feedback mechanisms within their platforms to enable customers to easily report suspicious activities, thereby closing the loop between awareness and real-time action.

Finally, collaboration between banks, telecommunication companies, academic institutions, and non-governmental organisations is essential to foster behavioural change. Joint campaigns guided by Protection Motivation Theory should focus on increasing both threat appraisal and coping efficacy among customers. Such multi-sectoral efforts are key to building a cybersecurity-conscious banking culture in Tanzania and across the region.

1. **Conclusion**

This study assessed the level of cybersecurity awareness among customers of NMB Bank Plc in Morogoro Municipality, Tanzania, in the context of the increasing adoption of digital banking services. The results revealed a considerable divide between general awareness of cybersecurity concepts and the practical application of protective behaviours. While most customers demonstrated awareness of the risks associated with sharing personal banking information and the consequences of cyber fraud, a significant proportion lacked confidence in identifying cyber threats and had not received any form of formal cybersecurity training. These findings underscore the pressing need for comprehensive and targeted cybersecurity education initiatives that go beyond basic information dissemination. The limited engagement with training and uncertainty in detecting threats suggest that customer awareness remains largely theoretical, leaving users and financial institutions vulnerable to cyberattacks. Furthermore, the study confirms that digital trust and safety are not solely technological concerns but also behavioural and educational challenges. The insights gained from this research contribute to the growing discourse on cybersecurity in developing economies, especially in the context of digital financial inclusion. For banks and policymakers alike, the emphasis must shift towards fostering a cybersecurity culture that empowers customers to take proactive roles in protecting their digital financial assets. Ultimately, improving cybersecurity awareness at the customer level is not only vital for individual protection but also for safeguarding the broader integrity and resilience of the financial system in Tanzania.

1. **Limitations and future research directions**

Despite providing valuable insights, this study is subject to several limitations that should be considered when generalising our findings. First, the research was geographically confined to Morogoro Municipality, which may limit the generalisability of the results to other regions of Tanzania or to different socio-economic contexts. Regional differences in digital literacy, banking infrastructure, and access to training could result in varied cybersecurity awareness levels across the country. Second, the study relied exclusively on self-reported data obtained through structured questionnaires. Such data are inherently susceptible to social desirability bias, where respondents may overstate their awareness or protective behaviours to align with perceived expectations. Additionally, while quantitative measures offered broad insights into awareness levels, they did not fully capture the nuances of customer behaviour and contextual understanding, which could have been enriched through in-depth qualitative methods such as interviews or focus groups. Third, the cross-sectional design of the study provides only a snapshot of cybersecurity awareness at a single point in time. This approach does not account for changes in awareness over time or the potential impact of evolving digital threats and educational interventions. Longitudinal research is needed to explore how awareness and behaviour shift in response to sustained training and policy changes. Lastly, the study did not differentiate awareness levels based on key demographic variables such as age, income level, or digital usage frequency. Understanding how these factors influence awareness would provide more targeted insights for designing effective interventions.

**COMPETING INTERESTS DISCLAIMER:**

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

**REFERENCES**

Bryman, A. (2016). *Social Research Methods* (5th ed.). Oxford University Press.

Choudhuri, D. S., Singh, A., Ravi, R., & Badhusha, M. (2024). An analysis of factors influencing consumer trust in online banking security measures. *Educational Administration: Theory and Practice*, *30*(2), 660-666. <https://doi.org/10.53555/kuey.v30i2.1742>

Cochran, W.G. (1977). *Sampling Techniques*, 3rd Ed., New York: John Wiley & Sons, Inc.

Creswell, J.W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Thousand Oaks, CA: Sage.

Dodge Jr, R.C., Carver, C., & Ferguson, A.J. (2007). Phishing for user security awareness. *Computers & Security*, *26*(1), 73-80. <https://doi.org/10.1016/j.cose.2006.10.009>

Milne, S., Sheeran, P., & Orbell, S. (2006). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106-143. <https://doi.org/10.1111/j.1559-1816.2000.tb02308.x>

Msambali, I.M., & Mwonge, L.A. (2025). Corporate social responsibility initiatives: strategies and mechanisms for promoting public health in Jordan University College in Morogoro Municipality, Tanzania. *Discover Health Systems*, *4*(1), 1-16. <https://doi.org/10.1007/s44250-025-00217-7>

Mwonge, L.A. & Naho, A. (2024). Evaluating the Smallholder Farmers' Perceptions Towards Agricultural Credit in Morogoro Municipality, Tanzania. *Business, Management and Economics: Research Progress* *5* (2024) 108-135, <https://doi.org/10.9734/bpi/bmerp/v5/1860>

National Microfinance Bank (NMB) (2020a). *Annual report: Cybersecurity and digital banking*. NMB Bank.

National Microfinance Bank (NMB) (2020b). Annual report: Cybersecurity risks and mitigation strategies.

National Microfinance Bank (NMB) (2024). Responsible Growth Lasting Impact: Sustainability Report 2024. <https://www.nmbbank.co.tz/images/documents/Sustainability_Report_2024.pdf>

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93-114. <https://doi.org/10.1080/00223980.1975.9915803>

Schutt, R.K. (2019). *Investigating the social world: The process and practice of research*. Sage Publications.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100. <https://doi.org/10.1016/j.compedu.2008.06.011>

Shukla, K., Ahmad, S., Bajpai, P., Srivastava, N., & Fatima, R. (2025). Assessing customer’s awareness of cybersecurity measurs in online banking: A study on digital trust and risk perception. *CINEFORUM*, *65*(2), 361-386.

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking Information Resource Cybersecurity System Modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), 80.

Suh, B., Han, I., & Han, B. (2017). Impact of trust, security and privacy in social networking: A cultural comparison. *International Journal of Human-Computer Studies*, *98*, 411-421.

United Republic of Tanzania (URT) (2017). National Microfinance Policy 2017. Ministry of Finance and Planning repository. <https://repository.mof.go.tz/handle/123456789/390>

Wamala, D., Mukisa, R., & Nyakaana, C. (2020). Cybersecurity policies and frameworks in Sub-Saharan Africa: The case of Uganda and Tanzania. *African Journal of Information Systems*, 12(1), 65–79.

Wang, S., Asif, M., Shahzad, M.F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & security*, *147*, 104051.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. <https://doi.org/10.1080/08874417.2020.1712269>