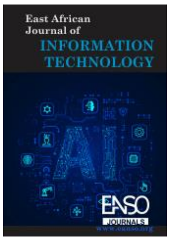


East African Journal of Information Technology
eajit.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar

Zedi Abdalla Khamis[1*]

[1] The State University of Zanzibar, P. O. Box 146, Zanzibar, Tanzania.
* Author's ORCID ID; https://orcid.org/0009-0006-8301-9269; Email: zediabdalla011@gmail.com

Article DOI: https://doi.org/10.37284/eajit.8.1.3010

Date Published:

16 May 2025

Keywords:

Information Security, Knowledge, Attitude, Behaviour, Mobile banking.

ABSTRACT

Mobile banking is becoming increasingly popular in Zanzibar. This study examines the information security knowledge, attitudes, and behaviours of mobile banking users in the region. A descriptive approach was employed with a quantitative research design. Data were collected from a sample of 95 mobile banking users in Zanzibar, as calculated using the Yamane formula based on the total population. The data collected through questionnaires was analysed using SPSS version 26. The analysis revealed that users have a moderate level of awareness concerning various cybersecurity risks associated with mobile banking. They recognised the importance of using strong passwords and understood that clicking on unknown links or attachments in emails could compromise their security. However, awareness was lower regarding the privacy risks of sharing personal information on social media. Additionally, the findings indicated that a moderate proportion of respondents acknowledged the risks associated with using public Wi-Fi for banking transactions. The study also found that participants had a moderate level of confidence in the effectiveness of two-factor authentication (2FA) for securing mobile banking. Moreover, most respondents moderately checked if a website was secure (e.g., HTTPS) before entering personal information. Based on these findings, the study recommends developing comprehensive information security awareness programs, utilising registered or recommended hardware and software to enhance security, maximising data protection against malware, improving the interactivity of mobile banking applications while addressing security concerns, and emphasising the usefulness and security features of mobile banking services in marketing efforts.

APA CITATION

Khamis, Z. A. (2025). Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar. *East African Journal of Information Technology*, *8*(1), 92-101. https://doi.org/10.37284/eajit.8.1.3010

CHICAGO CITATION

Khamis, Zedi Abdalla. 2025. "Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar". *East African Journal of Information Technology* 8 (1), 92-101. https://doi.org/10.37284/eajit.8.1.3010.

HARVARD CITATION

Khamis, Z. A. (2025) "Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar", *East African Journal of Information Technology*, 8(1), pp. 92-101. doi: 10.37284/eajit.8.1.3010

IEEE CITATION

Z. A., Khamis “Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar”, *EAJIT*, vol. 8, no. 1, pp. 92-101, May. 2025.

MLA CITATION

Khamis, Zedi Abdalla “Examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar”. *East African Journal of Information Technology*, Vol. 8, no. 1, May. 2025, pp. 92-101, doi:10.37284/eajit.8.1.3010

INTRODUCTION

The rapid advancement of financial technology has fundamentally transformed banking operations worldwide, with mobile banking emerging as a vital instrument for conducting financial transactions. Since its inception in the late 1980s, online banking has undergone substantial evolution, enabling users to execute transactions via electronic devices. Currently, mobile banking provides account holders with the convenience to transfer funds, settle bills, and manage their finances from virtually any location using smartphones and other mobile devices. The widespread adoption of mobile banking is primarily attributed to factors such as accessibility, user-friendliness, and a growing demographic of young users aged 18 to 32. Nonetheless, despite its numerous advantages, mobile banking is accompanied by significant security challenges.

Security concerns remain a prominent barrier to the widespread adoption of mobile banking, as users encounter various cyber threats, including malware, phishing attacks, key loggers, and ransomware (Wazid et al., 2019). The increasing dependence on digital transactions, expedited by the COVID-19 pandemic and rapid technological advancements, has contributed to a rise in cybercrime. Malicious actors exploit vulnerabilities within banking systems, legal inadequacies in cybersecurity enforcement, and users' insufficient awareness to perpetrate financial fraud (Stephen, 2021). In developing nations, such as Tanzania, mobile banking has played a pivotal role in promoting financial inclusion; however, security threats continue to pose risks to both users and financial institutions (Gupta et al., 2017).

The escalating sophistication of cyberattacks presents a significant challenge to banks and their clientele. Research indicates that Internet banking users are particularly vulnerable to cyber threats due to outdated security technologies, numerous entry points on the Internet, and a general lack of cybersecurity awareness (Suman & Sujata, 2020). Furthermore, variables such as users' educational levels, experience with mobile banking, and awareness of security risks greatly influence their susceptibility to cyber threats (Obadia, 2016). In the case of Zanzibar, it is crucial to comprehend mobile banking users' knowledge, attitudes, and behaviours regarding information security to develop effective strategies aimed at enhancing cybersecurity awareness and mitigating associated risks.

This study seeks to investigate the level of information security knowledge, attitudes, and behaviours among mobile banking users in Zanzibar. By evaluating users' awareness of security threats and their practices for safeguarding financial transactions, this research aims to elucidate the challenges faced by mobile banking users and propose measures to bolster cybersecurity awareness and protective measures within the banking sector.

Research Objective

The following were specific objectives of this study:

- To evaluate the knowledge of information security among mobile banking users in Zanzibar.
- To determine the attitude of information security among mobile banking users in Zanzibar.
- To analyse the behaviour of information security among mobile banking users in Zanzibar.

LITERATURE REVIEW

Definition of Key Terms

Information Security

Information security is a critical aspect of modern computing environments, influencing various aspects of daily life, including online learning, shopping, and banking (Whitman & Mattord, 2012). It encompasses the protection of information systems from unauthorised access, modification, and destruction. One widely recognised framework for information security is the CIA triad, which consists of Confidentiality, Integrity, and Availability (Andress, 2014). Confidentiality ensures that sensitive data is accessible only to authorised users, integrity safeguards information from unauthorised alterations, and availability ensures that information is accessible whenever needed (Arisya et al., 2020). These principles form the foundation of secure online transactions, including mobile banking.

Mobile Banking

Mobile banking refers to the use of mobile devices to perform banking transactions, including fund transfers, bill payments, and balance inquiries (Wazid, 2019). It serves as a convenient alternative to traditional banking, allowing users to manage their finances remotely. Research highlights mobile banking as an innovative communication channel that enhances financial accessibility and efficiency (Shaikh & Karjaluoto, 2015). However, despite its benefits, mobile banking is highly vulnerable to cybersecurity threats, making security awareness among users crucial.

Information Security Awareness

Information security awareness refers to an individual's understanding of cybersecurity threats and their commitment to following security policies, guidelines, and best practices (Kruger & Kearney, 2006). A strong security awareness culture is vital for preventing security breaches, as human error remains one of the weakest links in information security. Common areas of security awareness include data protection, password management, social engineering, and malware prevention (Arisya et al., 2020). Social engineering, in particular, exploits human tendencies to trust and assist others, making effective awareness programs essential in mitigating security risks. Without adequate security awareness, users are more susceptible to cyber threats, endangering both personal and organisational data.

THEORETICAL LITERATURE REVIEW

Knowledge-Attitude-Behaviour (KAB)

Kruger and Kearney (2006) developed a prototype model for measuring information security awareness, which is structured around three key dimensions: knowledge (what individuals know), attitude (what they think), and behaviour (what they do). These dimensions provide a comprehensive framework for assessing security awareness. Each dimension is further divided into six focus areas, which serve as the foundation for security awareness campaigns. Within these focus areas, additional subdivisions are made where appropriate. This model underscores the importance of evaluating security awareness holistically, considering not only users’ knowledge of security threats but also their attitudes toward security practices and their actual security behaviours. Given its structured approach, this prototype serves as a valuable framework for examining Information Security Knowledge, Attitude, and Behaviour among Mobile Banking Users in Zanzibar, guiding this study in analysing users' attitudes, behaviours, and knowledge in the context of mobile banking security.

Empirical Literature Review

Several studies have examined information security awareness in mobile banking and related fields:

Ramadhani et al. (2024) conducted an assessment of information security awareness utilising the Human Aspects of Information Security

Questionnaire (HAIS-Q), concentrating on users' knowledge, attitudes, and behaviours. The findings revealed that while users exhibited a robust understanding of security risks, their security-related behaviours, particularly in relation to email usage and mobile device security, were found to be inadequate.

Arisya et al. (2020) evaluated security awareness among mobile banking users employing the Knowledge-Attitude-Behaviour (KAB) model in conjunction with the Analytic Hierarchy Process (AHP) methodology. A survey comprising 210 respondents in Indonesia indicated a generally high level of security awareness at 83.32%. Nevertheless, the knowledge, attitudes, and behaviours pertaining to social media security were notably deficient, highlighting the urgent need for targeted interventions to enhance user awareness.

Limna et al. (2023) investigated the correlation between cybersecurity knowledge, awareness, and behavioural security practices among mobile banking users in Thailand. The research established that cybersecurity knowledge had a direct impact on security awareness, which subsequently influenced users' behavioural security decisions. The findings underscored the necessity for banks to adopt comprehensive cybersecurity strategies to safeguard their users.

Gharaibeh (2013) explored customer acceptance of e-banking and identified that low levels of IT literacy among users constituted a significant security risk. The study indicated that a lack of understanding regarding online banking security heightened customers' vulnerability to cyber threats, thereby diminishing trust in digital financial services.

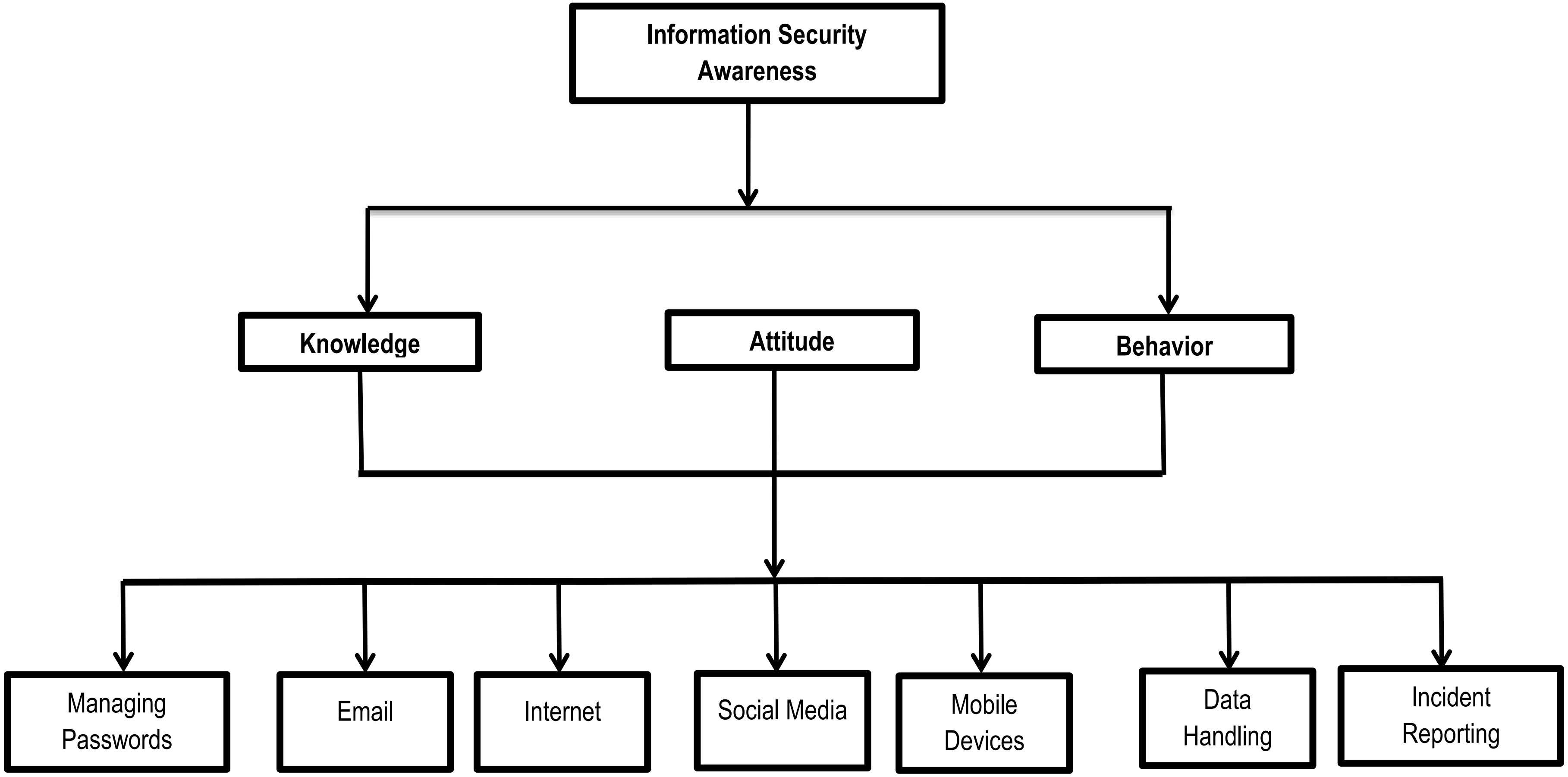
Du and Agami (2017) analysed perceptions of mobile banking security among young users. Their research revealed that while users recognised security threats, there was a significant reliance on banks to safeguard their accounts. A considerable number of users remained unaware of potential cyber threats, with authentication mechanisms identified as the most critical aspect of security.

Malero (2015) examined security awareness across different demographics of mobile money (M-Money) users in Tanzania. The study found that individuals with higher educational attainment and those aged 25 to 36 exhibited greater awareness of security risks. However, it also highlighted that reliance on simple authentication methods, such as PIN codes, left numerous users susceptible to fraud.

The Conceptual Framework

The study employed the KAB Theory. The major parts of the theories are Knowledge, Attitude, and Behaviour. The KAB model was applied to the seven measurements that refer to information security issues. Managing passwords, email, the internet, social media, mobile devices, data handling, and incident reporting make up the focal area. These parts construct the base on which the conceptual model is presented.

Figure 1. Conceptual Framework Source: Arisya et al., 2020



METHODOLOGY

This section presents the research design, sampling design, data collection, and analysis. A descriptive research design was used in this study. This study used a quantitative approach. As for this study, a simple random sampling technique was adopted to select a sample size. Therefore, this study adopted Yamane’s (1967) formula for sample size estimation.

$$n = \frac{\mathrm{N}}{1 + \mathrm{N}e^2}$$

Where n = Sample size, N = the population size (2000), e = is the random error (95%). By using the above formula, a sample size of 95 was obtained. In this study, Primary data were collected using a closed-ended questionnaire (Likert's Rating Scale) for data collection. The Likert scale used has 5 levels, starting from the lowest, namely strongly disagree, to the highest scale, which is strongly agreed. This questionnaire was created using the Google form platform, and the questionnaire has questions related to the KAB model, which was applied to the seven focus areas that refer to information security issues. Managing passwords, email, the internet, social media, mobile devices, data handling, and incident reporting make up the focal area. After the data collection was completed, the researcher analysed data obtained from questionnaires using descriptive statistics with the help of the Statistical Package for Social Sciences (SPSS). Descriptive statistics, such as frequencies, percentages, mean, and standard deviation, were primarily used to summarise the data.

RESULT

Descriptive Statistics

The respondents under study received 95 questionnaires, but only 94 questionnaires were returned and used for assessment. This represented 98.95% of the total. Using tables, major results from the research were presented.

Table 1: Descriptive Statistics

		Mean	Std. Deviation
To evaluate the knowledge of	Are you aware of the risks associated with reusing the same password across multiple accounts?	3.30	1.251
	Are you aware that clicking on unknown links or attachments in emails can compromise your security?	3.14	1.275
	Are you aware of the risks of conducting financial transactions over public Wi-Fi?	3.16	1.158
	Are you aware of the privacy risks of sharing personal information on social media?	2.90	1.345
	Are you aware of the importance of updating your device's operating system and apps for security purposes?	3.05	1.273
	Are you aware of the risks of sharing sensitive information, such as bank account details or passwords, with others?	3.13	1.229
	Are you aware of the importance of notifying your bank immediately if you lose your phone or suspect account compromise?	2.86	1.275
To determine the attitude of	How important is it to use a strong and unique password for each account?	2.74	1.436
	I respond to all e-mails that claim to be from the bank because I always believe the emails are from my bank.	2.46	1.114
	How concerned are you about the risks of using public Wi-Fi for banking transactions?	3.20	1.247
	How likely are you to avoid sharing personal information on social media due to privacy concerns?	3.23	1.425
	Is it possible for someone to steal my data through the internet and use it to steal money from mobile banking?	2.90	1.245
	Do you believe using two-factor authentication (2FA) for mobile banking is effective?	3.14	1.215

		Mean	Std. Deviation
To analyse the behaviour of	How much do you trust your mobile banking provider to protect your personal information?	2.88	.960
	How often do you change your mobile banking password?	2.98	.994
	Have you ever reported a phishing email or suspicious message to your email provider or bank?	2.39	1.070
	Do you check if a website is secure (e.g., HTTPS) before entering personal information?	2.74	1.015
	Have you adjusted your social media privacy settings to limit who can see your information?	2.88	1.269
	Do you regularly update your device's operating system and apps?	2.98	1.107
	How do you store sensitive information like PINs or account numbers securely?	2.96	1.235
	If you noticed a suspicious transaction on your account, how likely are you to report it immediately	3.07	1.157
	Composite Mean	**2.95**	

The statistical findings presented in the table above indicate that respondents have a moderate level of awareness regarding various cybersecurity risks associated with mobile banking. Specifically, a moderate proportion of respondents recognised the risks of reusing passwords (Mean = 3.30, SD = 1.251). Additionally, the study revealed that a majority of respondents were moderately aware that clicking on unknown links or attachments in emails could compromise their security (Mean = 3.14, SD = 1.275). Respondents also displayed a moderate level of awareness concerning the risks of conducting financial transactions over public Wi-Fi networks (Mean = 3.16, SD = 1.158).

Furthermore, most respondents acknowledged the importance of updating their device's operating system and applications for security purposes (Mean = 3.05, SD = 1.273). However, awareness was lower regarding the privacy risks of sharing personal information on social media (Mean = 2.90, SD = 1.345) and the necessity of notifying the bank in the event of a lost phone or compromised account (Mean = 2.86, SD = 1.275). On the other hand, a moderate number of respondents recognised the risks of sharing sensitive information, such as bank account details or passwords, with others (Mean = 3.13, SD = 1.229). Additionally, a similar level of awareness was reported regarding the requirement to inform the bank immediately about a lost phone or suspected account compromise (Mean = 2.86, SD = 1.275).

The findings also showed that a moderate majority of respondents acknowledged the importance of using strong and unique passwords for each account (Mean = 2.74, SD = 1.436). Nonetheless, a significant portion of respondents reported responding to emails claiming to be from their bank due to an inherent trust in such communications (Mean = 2.46, SD = 1.114). This finding suggests that some users may be vulnerable to phishing attacks.

Moreover, the study revealed a moderate proportion of respondents recognised the risks associated with using public Wi-Fi for banking transactions (Mean = 3.20, SD = 1.247). Respondents also expressed moderate concern regarding the sharing of personal information on social media due to privacy risks (Mean = 3.23, SD = 1.425) and the potential for cybercriminals to exploit internet vulnerabilities to steal money through mobile banking (Mean = 2.90, SD = 1.245).

Additionally, respondents reported a moderate level of confidence in the effectiveness of two-factor authentication (2FA) for mobile banking security (Mean = 3.14, SD = 1.215). However, their trust in their mobile banking provider's ability to protect personal information was relatively moderate (Mean = 2.88, SD = 0.960). The findings indicate that, to a moderate extent, users reported changing their passwords (Mean = 2.98, SD = 0.994). Yet, only a few users reported phishing emails or suspicious messages to their email provider or bank (Mean = 2.39, SD = 1.070). Nonetheless, the majority of respondents moderately checked if a website is secure (e.g., HTTPS) before entering personal information (Mean = 2.74, SD = 1.015), implying that users may have entered insecure websites, increasing the risk of data breaches.

DISCUSSION OF FINDINGS

The results indicate that respondents had a moderate level of cybersecurity awareness, especially about the dangers of clicking on unknown links or email attachments and reusing passwords. Golla et al. (2018) emphasise the necessity of user education regarding unique passwords and point out that password reuse presents risks if one database is compromised. The findings of this study revealed that a lot of people are ignorant of digital privacy and security procedures. Ben-Asher et al. (2011) highlight the disconnect between the need for mobile security and the shortcomings of existing safeguards, while Dawood et al. (2017) discovered that a lack of awareness can result in risky behaviours.

Since Meier et al. (2020) contend that more straightforward privacy policies can improve user comprehension, effective communication is essential. Even though some respondents are aware of the risks associated with disclosing private information, like bank account information, this awareness does not always translate into proactive action. With the popularity of mobile banking, it is essential to teach users how to report lost phones or suspected breaches.

All things considered, even though a lot of people understand the value of creating strong, unique passwords, this understanding frequently doesn't translate into safe practices. The propensity to respond to bank emails suggests susceptibility to phishing scams, highlighting the need for focused cybersecurity training. The study by Sarikakis and Winter (2017) indicates that users perceive privacy as control over their data, including sharing information with friends. Concerns about cybercriminals exploiting internet vulnerabilities for mobile banking theft align with Hong's (2019) findings, which highlight customer reluctance to adopt mobile banking technology.

The findings of this study revealed that users display moderate confidence in the effectiveness of two-factor authentication (2FA) for mobile banking security (Ali et al., 2021; Krol et al., 2015). Despite recognising 2FA's benefits, users maintain a moderate level of trust in mobile banking providers' ability to protect personal information, suggesting scepticism influenced by past experiences or media coverage of breaches (Jalali et al., 2020; Nilsson et al., 2005). While many users change their passwords, the low rate of reporting phishing attempts indicates a gap between passive security measures and proactive behaviours (Jalali et al., 2020; Parno et al., 2006). This emphasises a need for improved user education and reporting mechanisms (Khan et al., 2023; Tsai & Su, 2020).

Results of this study revealed that many respondents check if a website is secure only moderately, raising concerns about their awareness of website security. By not verifying website security (e.g., checking for HTTPS), users risk data breaches (Zhang et al., 2022). This finding contradicts the expectation that users prioritise data security when using e-government services (Shah et al., 2022). To address these issues, organisations should develop effective educational programs. As stated in Arain et al. (2019), online training can enhance understanding of IT security, while tailored interventions based on individual personality traits may improve user behaviour (Kennison & Chan-Tin, 2020).

CONCLUSION AND RECOMMENDATIONS

The study concludes that respondents have minimal knowledge of measures to secure themselves from information security knowledge, attitude, and behaviour use of mobile banking services in Zanzibar. To address this issue, mobile banking users need to be knowledgeable and aware of information security. Financial institutions should focus on enhancing users' information security knowledge, addressing perceived security concerns, and fostering positive attitudes towards mobile banking. Recommendations of this study include developing comprehensive information security awareness programs, using registered or recommended hardware and software can be advantageous, and maximising data protection from Malware, improving the interactivity of mobile banking applications while addressing security concerns, and emphasising the usefulness and security features of mobile banking services in marketing efforts.

REFERENCES

Ali, S., Khan, S., & Usman, M. (2021). Two-factor authentication for mobile banking: A study on user perception and effectiveness. *International Journal of Cyber Security and Digital Forensics, 10*(3), 201-215.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Arain, M. A., Tarhini, A., & Khan, S. (2019). Enhancing IT security awareness through online training programs: An empirical study. *Computers & Security, 84*, 15-26.

Arisya, F., Suryana, N., & Nugroho, A. (2020). Evaluating security awareness among mobile banking users using the knowledge-attitude-behavior model and analytic hierarchy process.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011). On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI).*

Dawood, H., Pournaghi, S. M., & Jøsang, A. (2017). The effect of user awareness on risky online behavior: An empirical study. *Computers & Security, 70*, 398-410.

Du, J., & Agami, N. (2017). Perceptions of mobile banking security: The case of young users in China. *International Journal of Mobile Communications, 15*(6), 620-644.

Gharaibeh, N. K. (2013). The adoption of e-banking: The case of Omani banks. *International Review of Management and Business Research, 2*(2), 600-615.

Golla, M., Krombholz, K., Hupperich, T., Holz, T., & Dürmuth, M. (2018). The password reset MitM attack: How to bypass account recovery in two-factor authentication. *27th USENIX Security Symposium.*

Gupta, S., & Arif, M. (2017). Adoption of internet banking service in Tanzania: The influencing factors. *University of Dar es Salaam Library Journal, 12*(2), 101-118.

Hong, W. (2019). Privacy and security concerns in mobile banking adoption: The role of trust and risk perception. *Journal of Information Security and Applications, 46*, 42-50.

Jalali, R., Siegel, M., & Madnick, S. (2020). Trust and security in online banking: Insights from customer behavior. *Journal of Cybersecurity, 6*(1), tyaa010.

Kennison, M., & Chan-Tin, E. (2020). Cybersecurity interventions and user behavior: The impact of personality traits on security practices. *Journal of Cybersecurity Education, Research and Practice, 5*(1), 7.

Khan, M. A., Alghamdi, N. S., & Khan, R. A. (2023). Phishing awareness and reporting behavior: The role of security training. *Journal of Cybersecurity Awareness, 15*(2), 125-138.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Krol, K., Moroz, M., & Sasse, M. A. (2015). Don't work for free: A theory of password security and user behavior. *Proceedings of the 11th*

Symposium on Usable Privacy and Security (SOUPS).

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology, 22*(140), 1-55.

Limna, C., et al. (2023). Correlation between cybersecurity knowledge, awareness, and behavioral security practices among mobile banking users in Thailand.

Malero, E. (2015). Security awareness among mobile money users in Tanzania. *International Journal of Computer Applications, 115*(6), 1-7.

Meier, F., Krombholz, K., Hupperich, T., Holz, T., & Dürmuth, M. (2020). Usability of privacy policies and controls in mobile applications. *Proceedings of the IEEE Symposium on Security and Privacy.*

Nilsson, A., Adams, A., & Herdman, J. (2005). Security and trust in online banking: A comparative study of user perceptions. *Financial Cryptography and Data Security.*

Obadia, A. (2016). Cyber security threats, vulnerabilities, and security solutions in the mobile banking sector.

Parno, B., Perrig, A., & Gligor, V. (2006). Distributed detection of node replication attacks in sensor networks. *Proceedings of the IEEE Symposium on Security and Privacy.*

Ramadhani, A., et al. (2024). Assessment of information security awareness using the human aspects of information security questionnaire (HAIS-Q).

Sarikakis, K., & Winter, L. (2017). Social media and privacy: The perception of control. *Media and Communication, 5*(1), 28-36.

Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and informatics*, 32(1), 129-142.

Shah, N., Patel, K., & Rathi, A. (2022). User awareness and security perceptions in e-government services: An analysis of security practices. *Government Information Quarterly, 39*(1), 101644.

Stephen, M. (2021). *Cyber security dynamics and usage of mobile banking services among commercial bank customers in Tanzania.*

Suman, G., & Sujata, M. (2020). Measuring user-perceived security of mobile banking applications. *arXiv preprint arXiv:2201.03052.*

Tsai, H. Y., & Su, C. (2020). Cybersecurity awareness and behavioral intentions: An empirical study on online users. *Computers in Human Behavior, 103*, 31-40.

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: Evolution and threats: Malware threats and security solutions. *IEEE Consumer Electronics Magazine, 8*(2), 56-60.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security*. Cengage Learning.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper and Row.

Zhang, X., Wang, Q., & Li, J. (2022). Evaluating website security awareness among online users: The role of HTTPS and security indicators. *International Journal of Information Security, 21*(4), 377-391.