GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.

MITIGATION OF RISK IN THE CONTEXT OF MOBILE BANKING IN GHANA

Stephen Oteng, Dr. Ashwinkumar A. Patel

PhD Scholar
Parul University, Gujarat India
Telephone Number: 23304355247
Email: stephen1442003@gmail.com

Assistant Professor
Parul University, Gujarat India
Telephone Number: 00919998980528
Email:ashwinkumarpatel528@gmail.com

Abstract

Mobile banking has revolutionised financial transactions, but its convenience comes with security concerns. This study investigates risks associated with mobile banking in Ghana and proposes mitigation measures. A mixed-methods approach was employed, collecting primary data through direct/physical and online questionnaires from 66 respondents. Eight risks were identified: misleading SMS/phishing scams, fake bank official calls, unauthorised access to accounts, mistaken money transfers, lost devices with saved banking details, login details stolen over WiFi/hotspots, delays in transaction confirmation, and identity verification scams. Results show a significant rise in fraud activity accompanying mobile banking adoption. Misleading SMS (39.34%) was the highest risk area. The study highlights the need for enhanced security measures, customer education, and robust authentication processes. Key Findings:39.34% of respondents received misleading SMS,66.67% used mobile banking, and 7.58% had never used internet banking. The study recommends that; banks enhance security, customer education, and authentication. Policymakers establish strict security standards and customer protection laws. This study contributes to the understanding of mobile banking risks in Ghana, informing stakeholders to mitigate these threats and ensure a secure financial environment.

Keywords: *Mobile banking, Security Risks, Financial transactions, Fraud Activity.*

INTRODUCTION

Mobile banking has gained popularity due to its convenience and instant access to financial information (Okiro & Ndungu, 2013). The proliferation of mobile devices has expanded mobile banking's reach. James C. (2020) defines mobile banking as making financial transactions on mobile devices. Before mobile devices, banks relied on physical branches. Today, new channels include mobile banking, ATMs, online help desks, call centres, and POS devices. Mobile banking has gained traction in Ghana, transforming how financial institutions interact with customers.

Mobile banking requires internet access and represents a breakthrough for remote banking services. Customers can now check balances, receive alerts, and make payments on their mobile phones. Distinguishing between mobile banking and mobile financial services is essential. Mobile financial services involve transferring money, marketing, banking, or payments using mobile devices, while mobile banking allows customers to conduct banking activities through a mobile phone (Okiro & Ndungu, 2013).

This paper focuses on mobile banking services, including SMS alerts, balance checks, mini statements, phone credit top-ups, intra-account transfers, and bill payments. Mobile banking offers a competitive advantage due to its 24-hour availability and reduced transaction costs.

To understand mobile banking risks, it is crucial to recognize the three common delivery mediums: Short Message Service (SMS), banks send financial information via SMS, vulnerable to misleading messages. Mobile-enabled internet browsers: Risky as online banking, with harder-to-use security features. Mobile applications: Introduces risks related to compromised or malicious software.

Mobile banking services are regulated, and banks invest heavily in security. However, various risks are associated with mobile banking. Key aspects of mobile banking include Convenience and 24-hour availability, reduced transaction costs, increased accessibility, risk of misleading SMS and phishing scams, vulnerability to compromised or malicious software, and regulatory compliance and security measures.

In Ghana, mobile banking has transformed the financial landscape. Addressing associated risks ensures a secure and reliable mobile banking environment.

GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.

HISTORY OF MOBILE BANKING

In the last four decades, the birth of the internet has facilitated the use of online banking. In the 1980s, the United American Bank started offering its customers home banking services. Remote banking services started in New York around 1981.

The history of mobile banking has its roots in the late 1990s and early 2000s and its introduction is strictly related to the boom of the internet. The first wireless application protocol (WAP) banking appeared in Norway in 1999. The Bank of Scotland indubitably is one of the global mobile banking pioneers. This bank in 2007 announced the world's first mobile banking app for smartphones. Also, Polish mobile banking pioneer Raiffeisen provided its customers with the first mobile application in 2004.

Ghana's mobile banking landscape began taking shape in 2009 with MTN's pioneering partnership with universal banks, followed by Airtel in 2010 and Tigo in 2012. Since then, the banking industry has undergone significant transformations, driven by technological advancements. Today, mobile banking has become a global phenomenon, with virtually every country embracing banking applications as an essential part of their financial ecosystem.

OBJECTIVE OF THE STUDY

The primary objective of this research is to examine the risks inherent in mobile banking services in Ghana and recommend practical measures to mitigate these risks.

THE PROBLEM STATEMENT

Mobile banking, a crucial factor in the banking industry's success, has been widely adopted by Ghanaian banks to serve their diverse customer base. However, despite its numerous advantages, mobile banking risks have emerged as a pressing concern for both banks and customers.

LITERATURE REVIEW

The Bank of Ghana's 2023 report reveals a 27.74% surge in attempted fraud cases in the banking and specialized deposit-taking institutions (SDI) sectors, from 2,347 in 2021 to 2,998 in 2022. However, the total loss value decreased by 7.88% to GH¢56 million in 2022, compared to GH¢61 million in 2021. Key drivers of fraud included document forgery, fraudulent withdrawals, cheque fraud, cyber/email scams, and cash theft.

In 2022, Payment Service Providers (PSPs) experienced a significant surge in electronic money-related losses, jumping 103% to GH¢26 million from GH¢12.8 million in 2021. Furthermore, cyber fraud cases skyrocketed by 744%, rising from 50 cases in 2021 to 422 cases in 2022. According to Serianu (2016), major mobile banking concerns include data breaches by external parties, insecure wireless network credential interception, unencrypted data, and reverse engineering risks. Separately, Mahad et al. (2015) noted that mobile devices have revolutionized banking, evolving from basic account management (balance checks, transaction views, and statement reviews) to complex transactions like fund transfers, bill payments, and loan applications.

Joubert and Belle (2013) found that rapid mobile technology advancements and high adoption rates in banking present significant growth opportunities, particularly in developing countries. However, He et al. (2015) noted a concerning trend: escalating mobile banking security threats over the past decade. This literature review highlights the risks inherent in mobile banking, which this paper aims to investigate.

METHODOLOGY OF THE STUDY

Primary data was used for collection of data for this study. Primary data was gathered through a questionnaire in two parts. The first part was the direct administration of a questionnaire to twenty (22) respondents at various points and this represents 33.33% of the total responses. The second part was an online questionnaire through email and WhatsApp. A total of forty-four (44) responses representing 66.67 of the total responses were received through WhatsApp, and out of this number, five (5) indicated that they had never used internet banking before. The table was used to analyze the data collected.

ANALYSIS OF THE RESULT

PRESENTATION OF THE DATA AND ANALYSIS

Table 1 below shows the data collected on the risks associated with mobile banking in Ghana. The total number of respondents to the questionnaire was sixty-six (66), and out of this number five (5) indicated that they had never used internet banking before. Their reason was that they did not have bank accounts.

GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.

Those who have never fallen victim to using internet banking were thirteen (13), and this represents 19.70% of the total responses received. Those who have fallen victim in one or the other way were forty-eight (48), and this also represents 72.73% of the total responses received. Those who have never used mobile before were five (5) and this represents 7.57% of the total responses received.

Twenty-four mobile banking users (39.34%) received misleading SMS messages that attempted to trick them into revealing their bank account details. Those who have never been victims of this were thirty-seven, and this also represents 60.66% of those who have used mobile banking before. This vulnerability represents the most significant risk associated with mobile banking, warranting urgent attention from banks, stakeholders, policymakers, and the government. The second most significant risk area involved phishing emails masquerading as bank communications, prompting users to take actions like password changes or resets.

The total number of responses that have been victims under this risk area was 21, and this represents 34.43% of the total responses received who have used mobile banks. The total number of respondents that have used mobile banking was sixty-one (61) and out of this number forty (40) representing 65.57% have never been victims in this risk area.

Based on the data received, the third highest risk area was, a call from someone purporting to be a bank official, needing to verify a customer login details to confirm an identity. Those who have been victims under this risk area were sixteen (16) representing 26.23% of the total respondents who have used internet banking before. Those who have not been victims under the risk area were forty-five (45) representing 73.77% of the total responses received who have used mobile banking before.

The fourth highest risk area was a bank customer mistakenly transferred money to someone. The total number that have been victims of this risk area was twelve (12) representing 19.67% of the total responses that have used mobile banking before. However, those who have not been victims under this risk area were forty-nine (49), and this represents 80.33% of the total responses that have used mobile banking before.

Unauthorized access by external parties to a customer's bank accounts through using login details that have been stolen directly from a mobile phone was the fifth highest risk area identified under those using mobile banking. Those who have been a victim under this risk area were eight (8), and this represents 13.11% of the total respondents who have used mobile banking before. The data also showed that 86.89% of the total respondents have never been victims of this risk area.

Misplaced or stolen devices with saved mobile banking details were also the sixth highest risk area based on the responses received. Those who have been victims under this risk area were four (4), and this represents 6.56% of those who have used mobile banking before. Those who have not been victims under this risk area were fifty-seven (57), and this represents 93.44% of the total responses received.

The last but not the least risk area identified was login details stolen over WiFi and hotspots of a bank customer. The total number of respondents who have been victims under this risk area was three (3) representing 4.92%. Those who have not been victims under this risk area were fifty-eight (58), and this also represents 95.08% of respondents who have used mobile banking before.

A customer indicated that he had a challenge making more than one transaction due to delays in the bank confirming a successful transaction. Another customer also mentioned that a scammer was able to detect his bank account details without his knowledge.

Table 1: Number of risks associated with mobile banking

	QUESTION	YES		NO		TOTAL
		Number	Percentage	Number	Percentage	
1	Receiving misleading short message service (SMS) that could prompt a customer to reveal bank account information	24	39.34%	37	60.66%	61
2	Unauthorized third parties gain access to a customer's bank accounts by using login details that have been stolen directly from mobile phone	8	13.11%	53	86.89%	61
3	Login details stolen over WiFi and hotspots of a bank customer	3	4.92%	58	95.08%	61
4	Misplaced devices that have mobile banking details saved in a text file	4	6.56%	57	93.44%	61
5	Phishing emails that appear to have come from a customer bank that include a call to take an action, such as a change or reset of password	21	34.43%	40	65.57%	61
6	A call from someone reporting to be a bank official, needing to verify a customer login details to confirm an identity	16	26.23%	45	73.77%	61
7	A bank customer mistakenly transferred money to someone	12	19.67%	49	80.33%	61

CONCLUSION AND RECOMMENDATIONS

Fraudulent mobile banking activities often go undetected until after the fact, eroding customer trust, especially among high-risk clients. The rapid growth of mobile banking has been matched by a surge in scams from individuals posing as bank representatives, as evidenced by this study and existing literature. To mitigate this risk, banks must prioritize customer education on mobile banking risks, while customers should take precautions like downloading banking apps from official websites and avoiding unsecured WiFi networks.

Customers should verify from their respective banks when they receive any messages or calls that are purported to come from their banks to take any action on their mobile banking application.

Banks must also put in place mechanisms that will ensure the safety of the use of mobile banking by customers. There are various safety measures which banks can put in place to curtail fraud associated with the use of mobile banking. These safety measures include; end-to-end encryption such as advanced encryption standard (AES), and full disk encryption solutions, encryption software that converts data into code, the banks should ensures mobile banking operations, banks should send short message service (SMS) notifications to the phone number of the customer on every transaction made, the use of biometric identity verification through thumb or facial verification, and finally customers should provide consent letters, for instance when transactions are above a certain threshold.

REFERENCES

[1] Bank of Ghana, (2023).Payment service providers' fraud report. https://www.bog.gov.gh› N...PDF

[2] He, W., Tian, X., and Shen, J.,(2015). Examining security risks of mobile banking.*Open Journal of Business and Management*, 12(4), 165-209.

[3] James, C. (2020). Mobile banking the implications and impact. *International Journal of Advanced Economics*, 8(6), 105-197

[4] Joubet N. and Belle, K. (2013). Mobile banking and its impact on financial service in Indonesia.*Strategic Management Journal*, 12(9), 567-601.

[5] Mahad, M., Mohtar, S., Yusoff, R. Z., and Othman, A. A., (2015). Factors affecting mobile adoption companies in Malaysia. *International Journal of Economics and Financial Issues*, 5 (3), 84-91.

[6] Okiro, K., & Ndungu, J., (2013). The impact of mobile and internet banking on the performance of financial institutions in Kenya. *European Scientific Journal,9*(13), 146-161.

[7] Seriano, M. (2016).Kenya cyber security report. Retrieved from.https://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf