ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

CLIENTS AWARENESS ON MULTI-FACTOR AUTHENTICATION IN BANKING SECURITY: BASIS FOR A PROPOSED CAMPAIGN DEVELOPMENT PROGRAM IN PREVENTING FINANCIAL FRAUD

Rosenda B Rañises MSCJ[1], Nida- Baligod Melad JD, MPA Ph. D can.[2]
Cromwell G Sanchez MSCJ[3], Asrakal K Dawai Ph. D can[4]
Mechelle Ibañez Yson MAED, LPT[5] , Michael Vher F Ilomin JD[6]

Article DOI: https://doi.org/10.36713/epra32141
DOI No: 10.36713/epra32141

ABSTRACT

This study examined the use of Multi-Factor Authentication (MFA) in banking security, focusing on the demographic profile, level of awareness, significant relationships, and challenges encountered by clients in preventing financial fraud. The findings revealed that most MFA users were aged 31–40 (34.2%), male (52%), married (57%), and college graduates (61%). Additionally, 45% conducted online banking transactions daily. Clients demonstrated moderate to high awareness of MFA in terms of online banking access, unauthorized access prevention, account recovery, and online fraud protection. However, awareness of account recovery procedures was comparatively lower. Statistical findings revealed significant relationships between clients' awareness and their age (p = 0.021), highest educational attainment (p = 0.013), and frequency of online transactions (p = 0.011). Meanwhile, gender (p = 0.351) and civil status (p = 0.431) showed no significant relationships. Furthermore, clients encountered challenges such as difficulties during setup, delayed one-time password (OTP) delivery, outdated registered devices, poor internet connectivity, limited technological familiarity, and unclear authentication instructions. The study concludes that although MFA strengthens online banking security and helps prevent financial fraud, its effectiveness depends on user awareness, accessibility, and system usability. It recommends continuous cybersecurity education, improved customer assistance, and more user-friendly authentication and account recovery mechanisms.

KEYWORDS: *Multi-Factor Authentication, Banking Security, Online Banking, Cybersecurity Awareness, Financial Fraud Prevention*

INTRODUCTION

Financial transactions have been transformed by the growing dependence on digital banking services, which provide clients with convenience and accessibility on a global scale. Nevertheless, the banking industry's adoption of digital transformation has resulted in a heightened level of cybersecurity threats, which poses substantial risks to financial institutions and their clients. In order to exploit vulnerabilities in online financial systems, cybercriminals employ sophisticated methods such as phishing, identity theft, and fraudulent transactions. In response to these threats, Multi-Factor Authentication (MFA) has emerged as a critical security measure, necessitating that users verify their identity using multiple authentication factors, including passwords, biometrics, or one-time passcodes.

MFA's success is contingent upon clients' cognizance and compliance, despite its efficacy in mitigating unauthorized access. Poor security practices may result from a lack of comprehension regarding MFA, rendering individuals more vulnerable to financial deception. This study investigates the extent to which clients are cognizant of multifactor authentication (MFA) in banking security and its potential impact on the development of a targeted campaign to improve fraud prevention.

The banking industry continues to grapple with the urgent issue of financial fraud, which is perpetrated by cybercriminals who capitalize on user negligence and inadequate security protocols. Many instances of unauthorized transactions are the result of compromised credentials, which could have been avoided through the proper implementation of MFA. Nevertheless, research indicates that clients' reluctance to implement MFA is rooted in misconceptions about its necessity, a lack of technical knowledge, or inconvenience. Furthermore, certain users unknowingly circumvent security features, rendering them vulnerable to fraudsters. The issue is not limited to individual banking clients; financial institutions are subject to regulatory penalties, financial losses, and reputational harm as a result of security breaches. Users' noncompliance and lack of awareness impede the efficacy of the stringent security measures that banks consistently implement. Consequently, it is imperative to evaluate clients' comprehension of MFA, pinpoint knowledge voids, and create an educational initiative that advocates for the most effective online banking security protocols.

LITERATURE REVIEW

Blancaflor et al. (2025) aawareness of the MFA varies considerably from a demography and geographic locations to

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

different demographic and geographic data, which prompted surveys on customer understanding of this safety measure and its implications for access and behavior of online banks. The urgency to adopt AMF practices is underlined by climbing the frequency of phishing attacks targeting banking networks, which serve as a gateway to cybercriminals to exploit vulnerable

accounts. In particular. Immerse yourself in the subtleties of advanced phishing techniques, highlighting the multifaceted challenges that customers encounter by recognizing and responding to such threats. This research indicates that without the adequate knowledge and understanding of the MFA, users can remain sensitive to attacks which could compromise their financial assets and their personal data.

Ramos et al. (2023) In the awareness of the client to the MFA within the Philippine banks, indicates that if certain customers perceive MFA as an essential security measure, there remains a widespread skepticism concerning its convenience. This duality of perception poses a challenge for banking institutions, because customers weigh compromise between security and user experience. Research highlights the need for banks to find a balance between the introduction of robust safety measures and the guarantee that customers feel confident and comfortable using these systems. Overall, the literature indicates a clear need for improved educational efforts and a better understanding of user attitudes towards the MFA to promote safer banking practices in a constantly evolving digital landscape., Multifatorial authentication (MFA) has been widely recognized as a crucial component for improving the safety of online bank systems. The effectiveness of MFA in preventing unauthorized access drew attention in several studies, particularly among the contributions of foreign research that analyze the implications for user behavior.

Samonte et al. (2025) provide a complete survey on the integration of MFA into electronic commercial platforms, revealing that consumer perception considerably influences the acceptance and efficiency of these security measures. Their research underlines that if customers recognize the importance of security protocols such as MFA, false ideas on their functionality and their necessity persist, which can hinder generalized adoption. This observation is essential, because it suggests that improving awareness and education for customers concerning MFA could serve as a central step to strengthen banking security against unauthorized access.

Feliciano and Reyes (2025) explored digital literacy levels within the Philippin banking sector, illustrating that a decrease in digital literacy can be correlated with the resistance to the adoption of security measures such as MFA. They postulate that initiatives aimed at improving digital literacy could considerably improve user engagement with MFA, ultimately resulting in a substantial reduction in risks associated with unauthorized access to financial services.

OBJECTIVES OF THE STUDY

This study aimed to assess the client's awareness on Multi-Factor Authentication in banking security to serve as basis for a proposed campaign development program in preventing financial fraud.

Specifically, it sought answers to the following questions:

1. What is the demographic profile of the clients who use the Multi-Factor Authentication in terms of:
    - 1.1. Age;
    - 1.2. Gender;
    - 1.3. Civil Status;
    - 1.4. Educational Attainment;
    - 1.5. Frequency of Online Transactions?
2. What is the level of awareness of clients on Multi-Factor Authentication in banking security in terms of:
    - 2.1. Online Banking Access;
    - 2.2 Unauthorized Access;
    - 2.2. Account Recovery; and
    - 2.3. Online Fraud?
3. Is there significant relationship between the demographic profile and level of awareness of clients on Multi-Factor Authentication in banking security?
4. What are the challenges encountered by the clients on using the Multi-Factor Authentication and preventing the financial fraud?
5. Based on the findings, what campaign development program can be proposed to prevent the financial fraud among clients of banking industry?

METHODOLOGY

This study adopted a quantitative research approach, specifically employing a descriptive survey and descriptive correlational design to assess clients' awareness of Multi-Factor Authentication (MFA) in banking security. The descriptive survey design is utilized to systematically gather data regarding the demographic profile of banking clients, including age, gender, civil status, educational attainment, and frequency of online transactions. This method enables researchers to obtain measurable and objective data that provide insights into trends and patterns among banking clients (Creswell & Creswell, 2023). By collecting information on these demographic factors, the study can identify potential influences on clients' awareness and utilization of MFA in securing their financial transactions.

In addition, the study examined the level of awareness of clients on MFA in banking security, specifically their understanding of authentication factors, familiarity with bank security protocols, perceived importance of MFA in financial security, and ability to recognize and prevent phishing and fraud attempts. The descriptive survey design ensures that this information is collected in a structured and quantifiable manner, allowing for statistical analysis of how well clients comprehend and engage with MFA security measures (Bryman, 2022). Given the increasing prevalence of cybercrimes, understanding these aspects is critical in identifying gaps in knowledge and potential areas for security enhancement.

A descriptive correlational design was also be employed to determine whether there is a significant relationship between clients' demographic profiles and their level of awareness of

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

MFA in banking security. This design is useful in identifying patterns and associations between demographic variables and clients' knowledge of authentication measures (Saunders et al., 2022). For example, it may reveal whether individuals with higher educational attainment are more aware of MFA security protocols or if frequency of online transactions influences a client's ability to recognize phishing attempts. Although correlational studies do not establish causation, they provide valuable insights that can inform targeted security awareness campaigns and policies.

By using this combined approach, the study aimed to generate meaningful data that can serve as a foundation for a proposed campaign development program in preventing financial fraud. The findings can help banking institutions, policymakers, and cybersecurity professionals design effective awareness programs tailored to different demographic groups. Ultimately, this study seeks to contribute to enhancing financial security measures and reducing vulnerabilities in online banking transactions by promoting greater awareness and adoption of MFA among clients (Babbie, 2021).

SCOPE AND DELIMITATION

This study focused on assessing clients' awareness of Multi-Factor Authentication (MFA) in banking security, serving as the foundation for a proposed campaign development program to prevent financial fraud. Specifically, the study examined the demographic profile of banking clients who utilized MFA, considering factors such as age, gender, civil status, educational attainment, and frequency of online transactions. Additionally, it evaluated the level of awareness regarding MFA in terms of understanding authentication factors, familiarity with bank security protocols, perceived importance of MFA in financial security, and ability to recognize and prevent phishing and fraud attempts. By analyzing these aspects, the study aimed to identify gaps in knowledge and challenges faced by users, providing insights for strengthening security awareness and fraud prevention measures in the banking industry.

The study was limited to Metro Manila, as this region has the highest concentration of banking institutions and digital banking users, making it a relevant setting for examining the extent of MFA awareness and cybersecurity threats. The respondents included clients who actively used MFA in online banking transactions, ensuring that the data collected reflects the experiences and challenges faced by those directly engaging with authentication mechanisms. The research was

conducted within the year 2025, allowing for an updated and relevant assessment of MFA awareness, particularly in the context of evolving cybersecurity threats and banking fraud tactics.

This study excluded individuals who do not use MFA in their banking transactions, as their lack of exposure to authentication security measures would not provide meaningful insights into the research objectives. Additionally, financial institutions, banking employees, and cybersecurity professionals are not included in the respondent pool, as the study focused solely on banking clients' perspectives and experiences. The study also does not cover other forms of online security measures outside of MFA, such as blockchain-based security or AI-driven fraud detection, keeping its scope strictly within the client's awareness and challenges related to MFA in banking security.

Data Gathering Tool

This study utilized a survey questionnaire as the primary research instrument for data collection. A structured survey is appropriate for gathering quantitative data, as it allows for the systematic collection of responses from multiple participants while ensuring consistency in the information obtained. The questionnaire was self-administered, meaning respondents answered the questions based on their personal experiences and perceptions regarding Multi-Factor Authentication (MFA) in banking security. This method ensures that data is collected efficiently while minimizing researcher bias in interpreting responses. The questionnaire was designed to be clear, concise, and easy to understand, enabling respondents from different demographic backgrounds to provide accurate answers.

The survey questionnaire was divided into two main parts. Part 1 focused on gathering information about the demographic profile of the respondents. It covered key variables such as age, gender, civil status, educational attainment, and frequency of online transactions. These demographic factors were essential in analyzing whether personal characteristics influence the level of awareness and challenges experienced in using MFA. By collecting this data, the study can determine potential correlations between user profiles and their understanding of cybersecurity measures in banking.

The questionnaire consisted of two subparts. The first subpart assessed the level of awareness of banking clients regarding MFA in banking security. This section included questions evaluating the respondents' understanding of MFA authentication factors, familiarity with bank security protocols related to MFA, perceived importance of MFA in financial security, and ability to recognize and prevent phishing and fraud attempts. Measuring awareness in these areas provided insight into whether users fully comprehend the role of MFA in securing their financial transactions and whether there are gaps in knowledge that need to be addressed through awareness campaigns.

The second subpart examined the challenges encountered by banking clients when using MFA and preventing financial fraud. This section identified common difficulties, such as technical issues, lack of understanding of authentication methods, inconvenience in the verification process, or susceptibility to cyber threats despite MFA implementation. By assessing these challenges, the study aims to uncover the barriers that hinder effective MFA adoption and propose necessary improvements to enhance security measures. The data gathered through the survey questionnaire served as the foundation for developing a campaign program that strengthens public awareness and improves cybersecurity practices among banking clients.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Data Gathering Procedures

The data collection process for this study followed a systematic approach to ensure accuracy and reliability in gathering information about clients' awareness and

challenges in using Multi-Factor Authentication (MFA) in banking security. Before the administration of the survey, the researcher sought approval from relevant institutions or authorities to conduct the study, ensuring compliance with ethical research standards. Once approval is granted, a pilot testing of the questionnaire was conducted with a small group of respondents to assess its clarity, relevance, and reliability. Necessary revisions were made based on feedback to enhance the instrument's effectiveness before full-scale distribution.

The survey questionnaire was then distributed to banking clients who utilized MFA in online banking transactions, using a convenience sampling technique to target respondents who were readily available and willing to participate. The questionnaire was administered physically or through an online platform to ensure accessibility and maximize response rates. Respondents were given clear instructions on how to answer the survey, and their participation was voluntary and confidential, with their personal information kept anonymous to maintain privacy and ethical integrity.

Once the data collection phase is complete, responses were organized and encoded for analysis. The demographic profiles of respondents were summarized using descriptive statistics, while the level of awareness regarding MFA was analyzed through mean scores and frequency distributions. Furthermore, correlational analysis was applied to determine if there was a significant relationship

between demographic factors and awareness levels. This analytical approach provided insights into potential patterns and gaps in MFA awareness among banking clients.

Finally, the findings had interpreted and documented to serve as the foundation for the development of a campaign program aimed at improving MFA awareness and preventing financial fraud. The results were presented in an organized manner, highlighting key trends, challenges, and recommendations. Ethical considerations, such as informed consent, voluntary participation, and data confidentiality, was upheld throughout the research process to ensure integrity and credibility in data gathering.

Ethical Considerations

During the study, Clients Awareness on Multi-Factor Authentication in Banking Security, numerous crucial ethical considerations were noted. All respondents, particularly the Clients, provided informed consent, demonstrating their voluntary involvement and comprehension of the study's objectives. Stringent protocols were implemented to preserve privacy and secrecy, safeguarding sensitive information. The study sought to mitigate harm, ensure equitable treatment of all respondents, and offer potential advantages to both people and society. When necessary, we secured ethical approval and ensured transparency throughout the research process. The findings were appropriately reported, and the respondents were provided with debriefing sessions. In summary, the study adhered to ethical norms by upholding integrity, respecting participants' rights, and complying with relevant rules.

RESULT AND DISCUSSION

Challenges Encountered by the clients on using the Multi-Factor Authentication and preventing the financial fraud

The Table 1 shows the Challenges Encountered by the clients on using the Multi-Factor Authentication and preventing financial fraud. Serious with an overall mean of 3.41. Most of the indicators are Serious. This are the following with their mean: "I struggle to access my account when the OTP is sent to a device, I no longer use" and "I can't always tell whether a message asking for my login info is real or a scam" both have a mean of 3.51; "I'm not fully aware of how multi-factor authentication protects me from financial fraud" has a mean of 3.50 considered as Very Serious. "I find it hard to get help from customer service when I have problems with MFA" and "I'm not always notified when someone tries to access my account without permission" both have a mean of 3.42; "I sometimes don't receive the one-time password (OTP) right away, which delays my transactions" and "I've disabled MFA before because I thought it wasn't necessary" both have a mean of 3.40; "I've experienced technical issues in my banking app that made MFA fail" has a mean of 3.39; "I'm not comfortable using authenticator apps or other security tools required by my bank" has a mean of 3.38; "I experience difficulties using MFA when my internet connection is weak" and "I sometimes avoid using MFA because it makes logging in more complicated" both have a mean of 3.37; "I find it confusing to set up multi-factor authentication on my online banking account" has a mean of 3.36; "I feel uneasy providing too much personal information when setting up MFA" has a mean of 3.35; "I find it hard to use MFA because I'm not very familiar with technology" has a mean of 3.34.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Table 1
Challenges Encountered by the clients on using the Multi-Factor Authentication and preventing financial fraud

INDICATORS	M	VI
I find it confusing to set up multi-factor authentication on my online banking account	**3.36**	**S**
I sometimes don't receive the one-time password (OTP) right away, which delays my transactions	**3.40**	**S**
I'm not fully aware of how multi-factor authentication protects me from financial fraud	**3.50**	**VS**
I struggle to access my account when the OTP is sent to a device I no longer use	**3.51**	**VS**
I experience difficulties using MFA when my internet connection is weak	**3.37**	**S**
I'm not comfortable using authenticator apps or other security tools required by my bank	**3.38**	**S**
I get confused when my bank changes the way MFA works without clear instructions	**3.41**	**S**
I find it hard to get help from customer service when I have problems with MFA	**3.42**	**S**
I sometimes avoid using MFA because it makes logging in more complicated	**3.37**	**S**
I feel uneasy providing too much personal information when setting up MFA	**3.35**	**S**
I can't always tell whether a message asking for my login info is real or a scam	**3.51**	**VS**
I've experienced technical issues in my banking app that made MFA fail	**3.39**	**S**
I find it hard to use MFA because I'm not very familiar with technology	**3.34**	**S**
I've disabled MFA before because I thought it wasn't necessary	**3.40**	**S**
I'm not always notified when someone tries to access my account without permission	**3.42**	**S**
Overall	**3.41**	**S**

Legend: M= Mean VI= Verbal Interpretation
3.50 – 4.00 = Very Serious (VS) 2.50 – 3.49 = Serious (S)
1.50 – 2.49 = Less Serious (LS) 1.00 – 1.49 = Very Serious (NS)

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Practical Implications

These are the conclusions formulated by the researcher after investigating the issue:

1. The findings reveal that clients who use Multi-Factor Authentication (MFA) come from diverse age groups, genders, civil statuses, educational backgrounds, and levels of online banking activity. However, those with higher educational attainment and who frequently perform online transactions tend to be more engaged and familiar with MFA. This suggests that education and digital exposure play an important role in influencing the use of MFA in banking.
2. Clients generally show a good level of awareness about MFA in terms of its importance in online banking access, preventing unauthorized access, aiding account recovery, and protecting against online fraud. They understand that MFA provides added security and plays a vital role in keeping their financial accounts safe during digital transactions.
3. There is a significant relationship between some demographic factors like age, educational attainment, and frequency of online transactions and clients' awareness of MFA. This means that individuals who are more educated and have more experience with online banking tend to have a better understanding of how MFA works and why it is important, while gender and civil status do not have a significant effect.
4. Clients face several challenges when using MFA, such as technical issues, delayed OTPs, difficulty accessing accounts from old devices, and confusion due to frequent changes in security processes. Some also struggle with internet connectivity or are not comfortable using technology. These issues can lead to frustration and may discourage clients from consistently using MFA.
5. Based on the findings, a campaign program should be developed that focuses on educating clients about MFA and addressing the challenges they face. The program should include user-friendly guides, customer support assistance, and digital literacy training, especially for less tech-savvy users. It should aim to build awareness, improve ease of use, and encourage consistent use of MFA to better protect clients from financial fraud.

Recommendations

Based on the conclusions of the study, the following recommendations are suggested to improve client awareness and the effective use of Multi-Factor Authentication in banking security.

1. Banks and financial institutions should implement targeted educational campaigns, especially for clients with lower educational attainment and limited digital experience. These campaigns can include webinars, in-app tutorials, and community outreach to promote understanding and usage of Multi-Factor Authentication (MFA).
2. Banks should regularly inform clients about the importance and functions of MFA in safeguarding online transactions.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

This can be done through email notifications, mobile app banners, and short video explainers that highlight how MFA protects against unauthorized access and online fraud.

3. Since awareness levels vary by age, education, and online activity, banks should adopt customized approaches to MFA implementation. For instance, tech-savvy users might prefer authenticator apps, while others may benefit from simpler OTP methods with clear instructions.
4. Financial institutions must streamline MFA processes to reduce confusion and technical barriers. This includes ensuring fast OTP delivery, offering multiple secure authentication options, improving customer service response times, and addressing connectivity concerns with offline alternatives where possible.
5. Develop and implement a client-centered campaign program focused on fraud prevention. It should integrate digital literacy training, scam awareness, and step-by-step guides on MFA usage. The program must prioritize inclusivity, ensuring all clients regardless of technical skill can confidently use MFA system

REFERENCES

1. *Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A framework integrating multi-factor authentication and Machine Learning. AI, 5(1), 177-194. https://www.mdpi.com/2673-2688/5/1/10*
2. *Ahmad, M. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). BAuth-ZKP – A blockchain-based multi-factor authentication mechanism for securing smart cities. Sensors, 23(5), 2757. https://www.mdpi.com/1424-8220/23/5/2757*
3. *Akinbowale, O. E., Mashigo, M. P., & Zerihun, P. (2024). Understanding and mitigating cyberfraud in Africa (p. 392). AOSIS. https://library.oapen.org/handle/20.500.12657/91185*
4. *Blancaflor, E. B., Duldulao, J. O., Espeño, J. V. E., Patag, G. S. M., Menor, M. T., & Intal, G. L. (2025). Advanced Phishing Techniques: Analyzing Adversary-in-the-Middle and Browser-in-the-Browser Attacks in Modern Cybersecurity. Cybernetics and Information Technologies, 25(1). https://sciendo.com/pdf/10.2478/cait-2025-0004*
5. *Esteban, A. P. (2023). Web engineering and e-commerce: Bridging technology and business in the Philippines. Nueva Ecija University of Science and Technology. https://books.google.com/books?hl=en&lr=&id=uKLUEAAAQBAJ&oi=fnd&pg=PA2&dq=Client+awareness+of+Multi-Factor+Authentication+in+online+banking+security+Philippines+and+abroad&ots=JBvR0f4WAZ&sig=LowVt_AnTKBdtvOBK8syUc8SuUY*
6. *Guma, A. (2022). Development of a secure multi-factor authentication algorithm for mobile money applications (Doctoral dissertation, NM-AIST).*
7. *Hossain, M. A., & Raza, M. A. (2023). Exploring The Effectiveness Of Multifactor Authentication In Preventing Unauthorized Access To Online Banking Systems. Multidisciplinary Science Journal, 1(01), 8- https://www.researchgate.net/profile/Mohammad-Hossain-201/publication/388314198_EXPLORING_THE_EFFECTIVENESS_OF_MULTIFACTOR_AUTHENTICATION_IN_PREVENTING_UNAUTHORIZED_ACCESS_TO_ONLINE_BANKING_SYSTEMS/links/679225be96e7fb48b998f489/EXPLORING-THE-EFFECTIVENESS-OF-MULTIFACTOR-AUTHENTICATION-IN-PREVENTING-UNAUTHORIZED-ACCESS-TO-ONLINE-BANKING-SYSTEMS.pdf*
8. *Khan, S. (2024). Enhancing User Trust in FinTech: A Multi-Factor Authentication Study. Journal of Applied Information Science, 12(2). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=23216115&AN=182787426&h=1pJjxizs2%2F6pNQzke2UY6RdPCcAs82Un9iaYfg3L5%2Bc2UJz5ULFJv4j0REc03dj5q63AU2udq40klhqir%2BQ1oQ%3D%3D&crl=c*
9. *Kibaya, P. (2023). Design of a multifactor authentication system for automated teller machines (Doctoral dissertation, The University of Zambia). https://dspace.unza.zm/handle/123456789/8108*
10. *Morake, T. A. (2021). A multi-factor authentication approach for e-banking. University of Johannesburg (South Africa). https://search.proquest.com/openview/bc389418353ea721712ea99e95861049/1?pq-origsite=gscholar&cbl=2026366&diss=y*
11. *Rodriguez, J. M. (2025). Analyzing the Risk Management at BDO Unibank during Post Covid-19–Navigating Financial and Operational Risks: A Case Study. https://www.preprints.org/manuscript/202504.0501*
12. *Samonte, M. J. C., Devera, J. T. O., Matoza, R. B. F., & Viernes, R. G. A. (2025). A Secure E-commerce Shopping Cart Design with Multi-factor Authentication, Tokenized Payment Processing, and Open-Source Integration for Enhanced User Experience and Reduced Development Time. In World Conference on Information Systems for Business Management (pp. 441-455). Springer, Singapore. https://link.springer.com/chapter/10.1007/978-981-96-1210-9_39*
13. *Talosig, B. M., & Teleron, J. I. Exploring Next-Generation Authentication: Strengthening Network Access and Security in the Digital Era. https://ijarasem.com/admin/img/20_Exploring%20Next.pdf*
14. *Umbach, R., Singh, A., & Walker, A. (2023). "Your Protection is in Your Hands Only": User Awareness and Adoption of Privacy and Security Practices in Five Majority World Countries. Journal of Online Trust and Safety, 2(1). https://tsjournal.org/index.php/jots/article/view/114*
15. *Bangko Sentral ng Pilipinas. (2022). Cybersecurity and Financial Fraud in the Digital Age. Manila, Philippines.*
16. *European Banking Authority. (2021). Multi-Factor Authentication and Fraud Prevention in Digital Banking.*
17. *Li, X., & Zhang, Y. (2022). User Awareness and Cybersecurity Measures in Online Banking: A Study on MFA Implementation in China. Journal of Financial Security, 10(2), 45-67.*
18. *National Privacy Commission. (2021). The State of Digital Security Among Filipino Banking Clients. Manila, Philippines.*
19. *Reyes, J., & Cruz, M. (2023). Challenges and Opportunities in Multi-Factor*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

20. *Authentication Adoption Among Filipino Banking Clients. Philippine Journal of Information Security, 8(1), 12-27.*
21. *Babbie, E. (2021). The practice of social research (15th ed.). Cengage Learning.*
22. *Bryman, A. (2022). Social research methods (6th ed.). Oxford University Press.*
23. *Creswell, J. W., & Creswell, J. D. (2023). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). SAGE Publications.*
24. *Saunders, M., Lewis, P., & Thornhill, A. (2022). Research methods for business students (9th ed.). Pearson*
25. *Smith, A., & Patel, R. (2023). Evaluating the Impact of Multi-Factor Authentication on Financial Fraud Prevention. Cybersecurity Journal, 15(4), 89-105.*
26. *Academia.edu. (2023). Exploring the effectiveness of multifactor authentication in preventing unauthorized access to online banking systems. Retrieved from https://www.academia.edu*
27. *Context PH. (2024). Philippine economy faces staggering $8.1 billion losses from online scams – report. Retrieved from https://context.ph*
28. *Inquirer. (2024). Alarming ₱460B lost to scams in PH, says study. Retrieved from https://newsinfo.inquirer.net*
29. *Neliti. (2024). Exploring the effectiveness of multifactor authentication in preventing unauthorized access and fraud. Retrieved from https://www.neliti.com*
30. *Statista. (2024). Most frequent consumer fraud schemes in the Philippines Q4 2024. Retrieved from https://www.statista.com*
31. *TransUnion. (2024). 2024 State of Omnichannel Fraud Report. Retrieved from https://www.transunion.ph*
32. *Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. Industrial Management and Data Systems, 121(3), 613-636. https://doi.org/10.1108/IMDS-08-2020-0462*
33. *Rao, A. S., & Rose, D. (2022). Continuous user authentication on smartphones via behavioral biometrics. Computers & Security, 112, 102489. https://doi.org/10.1016/j.cose.2021.102489*
34. *eMudhra. (2025). Dynamic Risk-Based Authentication in Banking Security. Retrieved from https://emudhra.com/en-us/blog/advancing-security-dynamic-risk-based-authentication-in-banking*
35. *Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039*
36. *Etikan, I., Musa, S. A., & Alkassim, R. S. (2023). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 12(2), 1-4.*
37. *Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A framework integrating multi-factor authentication and Machine Learning. AI, 5(1), 177-194.*
38. *Velásquez, I. (2021). Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication. Clei Electronic Journal, 24(1), 9-1.*
39. *Mahmood, R. K., Mahameed, A. I., Lateef, N. Q., Jasim, H. M., Radhi, A. D., Ahmed, S. R., & Tupe-Waghmare, P. (2024). Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. Journal of Robotics and Control (JRC), 5(5), 1502-1524.*
40. *Dahiya, P., & Kant, U. (2025). Multi-Factor Authentication Methods in Intelligent Systems. In Intelligent Manufacturing and Industry 4.0 (pp. 142-160). CRC Press.*
41. *Burton, S. L. (2025). Advancing cybersecurity: Strategic insights into multifactor authentication. Organizational Readiness and Research: Security, Management, and Decision Making, 247-282.*
42. *Das, S. (2020). A risk-reduction-based incentivization model for human-centered multi-factor authentication. Indiana University.*
43. *Moepi, G. L., & Mathonsi, T. E. (2023). Implementation of an Enhanced Multi-Factor Authentication Scheme with a Track and Trace Capability for Online Banking Platforms.*
44. *Mishra, K., Kaur, A., Kaushal, N., Kaur, S., Singh, N. T., & Bansal, S. (2024, June). A Regulatory Framework for Improving E-banking Security. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.*
45. *Kantipudi, R., Mallavarapu, A. S. K., Rajagopal, S. M., & Kagolanu, M. (2024, January). A Comprehensive Analysis on using Multifactor Authentication System for Three Level Security. In 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 498-503). IEEE.*
46. *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.*
47. *Khan, S. (2024). Enhancing User Trust in FinTech: A Multi-Factor Authentication Study. Journal of Applied Information Science, 12(2).*
48. *Kimani, C. W. (2022). Developing a multi-factor authentication prototype for improved security of enterprise resource planning systems for Kenyan universities (Doctoral dissertation, Africa Nazarene University).*
49. *Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A framework integrating multi-factor authentication and Machine Learning. AI, 5(1), 177-194.*
50. *Al-Sahli, R. A., Al-Mutairi, A., & Nasr, K. (2024). Secure Authentication System based on Multi-Factor Authentication. Taibah University. doi, 10.*
51. *Carrillo-Torres, D., Pérez-Díaz, J. A., Cantoral-Ceballos, J. A., & Vargas-Rosales, C. (2023). A novel multi-factor authentication algorithm based on image recognition and user established relations. Applied Sciences, 13(3), 1374.*
52. *Tolbert, M. (2021). Vulnerabilities of multi-factor authentication in modern computer networks. UK: Worcester Polytechnic Institute Worcester.*
53. *Das, S. (2020). A risk-reduction-based incentivization model for human-centered multi-factor authentication. Indiana University.*
54. *Nkubito, E., & Mbanzabugabo, J. B. (2024). The Legitimacy of Online Banking Transactions as a Value-Added Tool in Rwanda's Banking System. Open Access Library Journal, 11(12), 1-15.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 11| November 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

55. *Fanti, M. (2023). Implementing Multifactor Authentication: Protect your applications from cyberattacks with the help of MFA. Packt Publishing Ltd.*
56. *Brodahl, M., Flaathen, E. E., & Gigstad, M. C. (2024). Multi-factor Authentication in Tactical Systems (Bachelor's thesis, NTNU).*
57. *Guma, A. (2022). Development of a secure multi-factor authentication algorithm for mobile money applications (Doctoral dissertation, NM-AIST).*
58. *Samonte, M. J. C., Callejo, J. K., Lumbera, D. C. N., & Ocaya, J. C. B. (2024, August). Mitigating Vishing in Digital Banking Through Caller Authentication and*
59. *Verification Technologies. In 2024 14th International Conference on Software Technology and Engineering (ICSTE) (pp. 102-108). IEEE.*
60. *Talosig, B. M., & Teleron, J. I. Exploring Next-Generation Authentication: Strengthening Network Access and Security in the Digital Era.*
61. *Umbach, R., Singh, A., & Walker, A. (2023). "Your Protection is in Your Hands Only": User Awareness and Adoption of Privacy and Security Practices in Five Majority World Countries. Journal of Online Trust and Safety, 2(1).*
62. *Ahmad, M. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). BAuth-ZKP – A blockchain-based multi-factor authentication mechanism for securing smart cities. Sensors, 23(5), 2757.*
63. *Abduhari, E. S., Shaik, T. C., Adidul, A. B., Ladja, J. H., Saliddin, E. S., Adin, A. J., ... & Tahil, S. K. (2025). Access Control Mechanisms and Their Role in Preventing Unauthorized Data Access: A Comparative Analysis of RBAC, MFA, and Strong Passwords. Natural Sciences Engineering and Technology Journal, 5(1), 418-430.*
64. *Samonte, M. J. C., Ibarreta, M. V. O., Ilagan, K. A. A., & Justo, A. R. L. (2024, September). Mitigating Risk in the Digital Age: An Analysis of Security Measures for Cashless Payments in Developing Countries. In 2024 4th International Conference on Computer Systems (ICCS) (pp. 186-191). IEEE.*
65. *ITING, R. L., ISAHAC, L. M., AJURAM, M. J., KIMAR, J. D., AWAD, S. A., SALAHUDDIN, D., ... & LATORRE, N. J. (2024). UNDERSTANDING THE CRITICAL ROLE OF INFORMATION ASSURANCE IN MITIGATING CYBERCRIME RISKS.*
66. *Binaluyo, J. P., Santos, A. R., & Agustin, N. B. (2024). Challenges and opportunities for digital transformation in Philippine microfinance institutions. International Journal of Economics and Financial Issues, 14(5), 269-278.*
67. *Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A., & Pitchan, M. A. (2021). A systematic literature review of the types of authentication safety practices among internet users. International Journal of Advanced Computer Science and Applications, 12(7).*
68. *Guma, A. (2022). Development of a secure multi-factor authentication algorithm for mobile money applications (Doctoral dissertation, NM-AIST).*
69. *Esteban, A. P. (2023). Web engineering and e-commerce: Bridging technology and business in the Philippines. Nueva Ecija University of Science and Technology.*
70. *Gupta, S. (2025). Hacking the System: A Deep Dive into the World of E-Banking Crime. The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0, 121-148.*
71. *Talosig, B. M., & Teleron, J. I. Exploring Next-Generation Authentication: Strengthening Network Access and Security in the Digital Era.*
72. *Samonte, M. J. C., Ibarreta, M. V. O., Ilagan, K. A. A., & Justo, A. R. L. (2024, September). Mitigating Risk in the Digital Age: An Analysis of Security Measures for Cashless Payments in Developing Countries. In 2024 4th International Conference on Computer Systems (ICCS) (pp. 186-191). IEEE.*
73. *Liu, X. M. (2021). A risk-based approach to cybersecurity: a case study of financial messaging networks data breaches. The Coastal Business Journal, 18(1), 2.*
74. *Ahmad, M. O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). BAuth-ZKP – A blockchain-based multi-factor authentication mechanism for securing smart cities. Sensors, 23(5), 2757.*
75. *Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. World Journal of Advanced Research and Reviews, 21(3), 625-643.*
76. *Akinbowale, O. E., Mashigo, M. P., & Zerihun, P. (2024). Understanding and mitigating cyberfraud in Africa (p. 392). AOSIS.*
77. *Blancaflor, E. B., Abaleta, R. M., Achacoso, L. M. D., Amper, A. C. C., & Ampiloquio, P. I. R. (2024, September). Emerging Threat: The Use of AI Voice Cloning Software and Services to Deceive Victims Through Phone Conversations and its Potential Effects on the Filipino Population. In Proceeding of the 2024 5th Asia Service Sciences and Software Engineering Conference (pp. 137-146).*