Texila International Journal of Academic Research
ISSN: 2520-3088
DOI: 10.21522/TIJAR.2014.12.01.Art013

The Price of Transparency: How Exposing Personal Information in Mobile Money Transactions Fuels Social Engineering in Ghana

Daniel Adjei Odai
Department of Computer Science, Texila American University, Georgetown, Guyana

Abstract

Communications technologies such as 2G, 3G, 4G and 5G define a significant portion of today's cyberspace and has attracted innovative value-added services and financial technologies such as mobile money (MM) transactions. The success of MM introduction in Kenya has significantly influenced its global adoption in other developing countries, such as Ghana. While MM systems are widely studied for their economic transformation impact within the Ghanaian context, this paper hypothesised that, there is limited research on its contribution to widening the attack surface of social engineering (SE) attacks as a result of its exposure of personally identifiable information (PII) during transactions. The paper explored the hypothesis with a quantitative methodology adopted with primary data collected through questionnaires designed to capture user experiences, perceptions, and insights on privacy and security concerns during MM transactions. The findings confirmed the hypothesis: 96.7% of respondents acknowledged that their PII is visible to recipients during transactions, and 76.7% believed this exposure increases their vulnerability to scams. Additionally, 48.3% reported experiencing phishing attempts or suspicious behaviour where their PII was referenced after MM transaction.

Keywords: *Cyberspace, Mobile Money, PII, Social Engineering.*

Introduction

The evolution of cellular technology has rigorously gone through a remarkable transformation from the initial less complicated service rendering second generation technology(2G) to the more contemporary advanced fifth generation technology(5G) that underpins today's thriving mobile communications landscape. These communications technologies define a significant portion of today's cyberspace and has attracted innovative value-added services and financial technologies such as mobile money transactions. It's worth noting that, the growth of mobile technology has led to the development of various cashless transaction options worldwide [1]. Mobile money gained global prominence, particularly, after its introduction in Kenya as M-PESA [2]. The success of M-PESA has significantly influenced the adoption of mobile services in other developing countries, such as Ghana.

While mobile money systems are widely studied for their economic transformation impact within the Ghanaian context, there is limited research on its contribution to widening the attack surface of social engineering (SE) attacks as a result of its exposure of personally identifiable information (PII) during transactions. This gap arises as a result of exposure of PII, such as full names linked to mobile numbers, during transactions in the name of transparency. Quite notably, the ease with which users could have access to names associated with phone numbers, either through completed transactions or preliminary attempts, has been largely overlooked in existing studies. This paper identifies this aspect of the mobile money transaction processes as overlooked and it poses a considerable risk such as identity

Received: 19.01.2025 ***Accepted: 24.01.2025*** ***Published on: 31.01.2025***
****Corresponding Author: adjeido@gmail.com***

theft, impersonation fraud, and unauthorised data harvesting.

Reconnaissance is an important aspect of military planning operations because it strategically helps to understand the enemy. The reconnaissance operation systematically involves identifying and analysing the potential target in order to exploit its weaknesses [3]. For instance, in a likened case study, reconnaissance was carried out to measure security awareness of employees by revealing discrepancies between their understanding and actual behaviour during penetration in a penetration test. This highlights the importance of reconnaissance in identifying and exploiting human vulnerabilities [4]. Moreover, in [5], reconnaissance is regarded as a critical phase in the cyber kill chain, where adversaries gather information to exploit vulnerabilities in systems and people; this phase is essential for the success of subsequent attacks. Building on this, this paper further theorises that, the mobile money (MM) platforms in Ghana might be increasing the reconnaissance surface for information gathering.

A quantitative methodology was adopted with primary data collected through questionnaires designed to capture user experiences, perceptions, and insights on privacy and security concerns during MM transactions. This research though is region-specific and localised, it is intended to add unique knowledge to a global discourse on SE within the context of mobile money transactions security.

The PII Concept

Our online digital footprints, could be likened to secret keys that qualifies to be used to unlock personal information about us, be it our name, location, phone number, preferences and the rest. With the advent of personal data breaches and its antecedent cyber security concerns, Personally Identifiable Information (PII) has assumed a centre stage in data protection discussions due to its implications for individual privacy and the security of sensitive data. In [6], PII is defined as any information that can be used independently or in combination with other information to identify an individual; and the paper further highlighted the components of PII as names, social security numbers, dates and places of birth, MAC addresses, phone numbers and other identifiers that can trace an individual's identity. The growing importance of PII could be attributed to the rise of digital technologies and the increasing amount of personal data collected by organisations across wide range sectors of our daily lives, i.e., from online games, healthcare, finance, social media, e-commerce and the rest [7]. The need for robust protection measures regarding PII is adequately emphasised in existing literature, largely driven by concerns over data breaches and identity theft. Privacy is not merely a personal concern but a societal issue, where the misuse of PII can lead to significant harm, including financial loss, reputational damage, or potential social manipulation [8].

Various dimensions of PII protection, from legal frameworks to technological solutions are continuously being explored by researchers. Regarding legal frameworks, the "European Union’s (EU) General Data Protection Regulation (GDPR)" represents a landmark legal initiative aimed at strengthening the protection of PII that mandates explicit consent for data collection and providing individuals with the right to access, correct, and delete their personal data [9].

Ghana's data protection act, 2012(Act 843) is a legislation that plays an important role for protecting individual data and privacy. The legislation establishes the “Data Protection Commission (DPC)”, which is responsible for regulating the processing of personal information and ensuring individuals' privacy rights are upheld. The role of DPC in Ghana compares to the GDPR's tenets regarding safeguarding individuals PII against digital crimes [10].

The use of technology to tackling the challenges of PII is also an ongoing approach being explored by researchers. Quite a number of technological approaches such as cryptographic methods, data anonymisation, pseudonymisation, and encryption have all been put forward as effective techniques to protecting PII from unauthorised access. However, as challenges associated with PII evolves in complexity, some scholars have argued that these enumerated approaches are quite insufficient at addressing the emerging risks. It is argued that artificial intelligence algorithms especially in the domain of machine learning have the capability of de-anonymising data through pattern recognition thereby making traditional anonymisation techniques less effective [11].

Quite a number of gaps could be identified in current technological approaches to managing and securing PII. Firstly, while data masking is widely utilised to securing PII, it often results in inefficiencies during data analysis. Moreover, the application of machine learning systems at securing PII is bedevilled with notable error rates, particularly when these systems are employed across various regions. Additionally, although encryption and masking techniques are essential for enhancing data security, they introduce complexity and elevate costs associated with data transactions. Furthermore, traditional manual methods for tagging and securing PII are becoming increasingly impractical due to the sheer volume of data generated today. Lastly, there is a pressing demand for cost-effective automated techniques that require minimal data transformation while still providing strong security and privacy for PII [12].

Social Engineering

Social engineering (SE) is conceptually not technical in nature but rather leverage manipulating humans who are perceived to having what the attackers are in search of by persuading the target to unknowingly make available sensitive data or inadvertently aid the attack by performing certain actions [13] [14]. A plethora of methodologies and tactics are employed by attackers in their successful SE trade. All these SE attacks are performed based on harvested personal information of victims.

The risks associated with breach of personal information could range from minor disturbances to serious threats. However, this very personal data could also be leveraged to improve services, streamline interactions, and facilitate communication with interactive systems. Ironically, interactive systems are increasingly being designed with personal information as a critical element in areas such as e-commerce, healthcare, office work, and personal communications; this is a fundamental challenge [15].

The mobile Money platforms, this paper believes increases the attack surface for harvesting personal information. By design, the objective of SE attacks is basically to get hold of sensitive data, including PII, from their target.

In [16], a detailed classification system for social engineering attacks were presented as structured around several key components. Notable amongst them is the attack scenario class in which SE attacks could take place over multiple channels including human or software operators. Additionally, attacks could be classified into physical, technical, social, or socio-technical. The human factor channel has notoriously gained popularity in recent times.

In an annual Internet Crime Report for 2023, the FBI's Internet Crime Complaint Centre (IC3) made known phishing as the most frequently reported crime. The report pointed out a record number of complaints (i.e., 880,418) with potential losses exceeding $12.5 billion. Phishing/Spoofing accounted for over 34% of all the complaints [17]. This highlights the prevalence of phishing where attackers impersonate legitimate individuals or entities through the channels earlier enumerated to gain unauthorised access to sensitive data; this calls for action to minimise the attack surface.

Phishing

Phishing is described as an attempt at acquiring sensitive information such as usernames, passwords, and credit card details by perpetrators masquerading as trustworthy entities in an electronic communication. The approaches employed often involve communication that appears to be from a reputable source such as social media sites, auction platforms, or IT administrators, basically aimed at deceiving the unsuspecting individual [18, 19]. Notably, researchers have increasingly been focusing on understanding the mechanisms, psychological factors, and defence strategies against phishing in recent times. At the genesis of all of these, phishing attacks were primarily executed via email channels but contemporarily, phishing has extended to various digital platforms, including social media, SMS (smishing), and phone calls (vishing).

Role of PII in Phishing

Phishing is considered as a cybercrime activity that exploits PII, with the objective of deceiving individuals into giving away sensitive data. In [20] names and phone numbers were identified as PII, and PII theft was described as the unlawful acquisition of such PII qualifiers for malicious economic gain. Phishing kits are often used in attempts to gather PII such as email addresses, passwords, geolocation, and phone numbers. This highlights the significance of PII in phishing expeditions [21]. Additionally, the use of fake emails, websites, and messaging are among the channels commonly employed by phishers to masquerade as trusted sources, thereby tricking their victims into unknowingly providing their PII [22].

Materials and Methods

Research Design

This study adopted a quantitative research design to systematically investigate the exposure of personally identifiable information (PII) during mobile money transactions and its implications for social engineering attacks in Ghana. For its ability to provide reliable measurable data that effectively allows for statistical analysis and inferred generalisation, the quantitative approach was chosen. To align positively with the paper’s objective, the following quantifiable key variables were the focus of the design i.e., user awareness, perceptions of vulnerability, and recommendations for privacy improvements.

Research Instruments

An online questionnaire was used as the primary research instrument for data collection. The questionnaire was designed to include both closed-ended and multiple-choice questions. Key questions were focused on:

1. Awareness of PII exposure during mobile money transactions.
2. Perceived vulnerability to scams and attacks due to PII exposure.
3. User preferences for privacy-preserving features in mobile money platforms.
4. Opinions on the adequacy of public awareness campaigns addressing social engineering risks.
5. Recommendations for mitigating mobile money fraud and social engineering attacks.

Table 1. Summary of Key Questions Relevance

Question	Purpose & Relevance
Are you aware your full name and phone number are visible to any recipient in mobile money transactions?	To assess users’ foundational level of awareness about PII exposure during mobile money transactions.

Do you think the exposure of your full name and phone number during mobile money transactions makes you more vulnerable to scams or attacks?	To evaluate users' perceptions of how PII exposure increases their susceptibility to scams and social engineering attacks.
Would you feel safer if your mobile money transactions did not expose your full name and phone number to the recipient?	To understand users' preferences for privacy-preserving features in mobile money platforms.
Do you think that there is enough public awareness about the risks of social engineering and scams related to mobile money?	To gauge the perceived adequacy of public education and awareness campaigns addressing mobile money-related risks.
What do you think is the most effective way to prevent mobile money fraud and social engineering attacks in Ghana? (Select one or more options)	To identify user-driven recommendations for mitigating mobile money fraud, such as improved privacy measures or education.

Table 1 is a summary of the relevance of the key questions posed.

Data Collection Procedure

Electronic data collection procedure was used by leveraging digital platforms to distribute a questionnaire. This data collection method was adopted because of its efficiency, scalability, and accessibility at allowing respondents to participate at their convenience. Appropriately, this approach is quite effective at reaching the technologically adept target group and minimising logistical costs. Basically, research findings should be generalisable to the population from which the sample is drawn i.e., the sample must accurately represent the population [23]. In Ghana, online activities are largely driven by Subscriber Identity Module (SIM) card and the market share per operator is represented as 75%-MTN, 15%-Telecel, and 10%-AT [24]. These values, largely align with the distribution of questionnaire respondents per operator to which mobile money platform (MMP) respondents are on i.e., 68.90%-MTN, 23%-Telecel, 4.9%-AT, and 1.6%-GCB Mobile Money. It is worth noting that, users legitimately have multiple SIM cards and could opt for any MMP usage at any time convenient.

The use of paper-based forms for data capturing and subsequent entry into an electronic system is traditionally well established. On the other hand, it is quite easier to engage real-time data capture and analysis electronically. Largely, electronic data capture systems offer greater time efficiency and also enhance accuracy compared to paper-based methods [25].

Results & Discussion

MM & Personal Data Harvesting

For household garbage collection, this author relies on a private service provider that is not a registered entity and is unknown to the state. This type of service provider is common within the Ghanaian community. In the event of any incident where the service provider might be implicated, how would the state be able to trace this unregistered entity? To gain access to their contact information, I initiated a feigned payment through mobile money, which required the service provider to granted me their phone number. Once I had the number, I was easily able to retrieve the associated full name through the mobile platform. This demonstrates how easily personal data, such as mobile numbers and accompanying names, could be collected via mobile money services.

Age Group

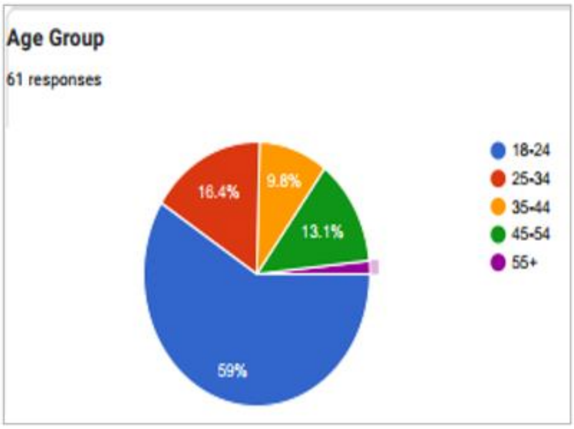


Figure 1. Age Group

The questionnaire garnered 61 responses with one not a user of MM service. 85.2% of the respondents were in the age group of 18-44 as in Figure 1 above.

As pointed out in [26], familiarity with technology varies quite significantly across age groups; usually, younger generations favour interactive media and online platforms for information and entertainment based on their acquired digital skills. In contrast, older generations go for traditional media due to lower digital literacy [27]. This implies that, drivers of mobile money growth in Ghana are the youth.

MM Usage Frequency

User behaviour, dependence on MM platform, potential exposure to SE risk, and likelihood of targeted vulnerability were put to test as captured in Figure 2 below.

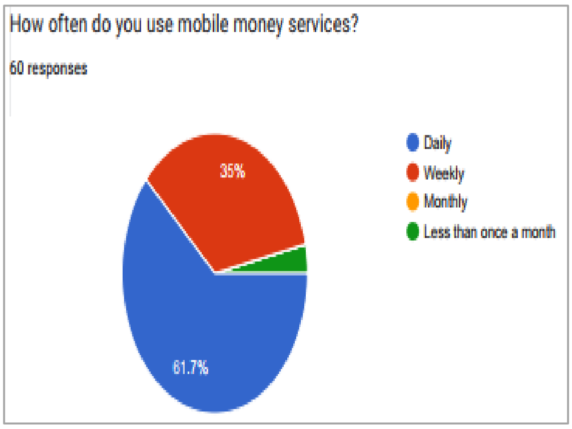
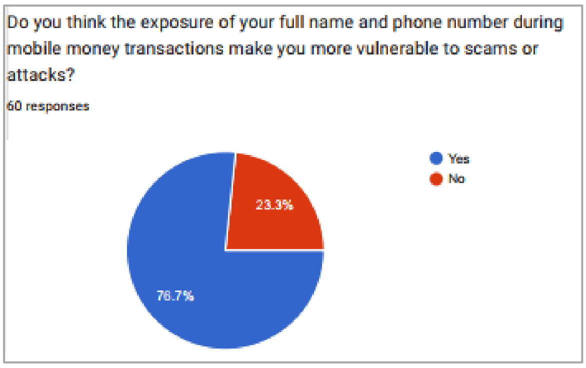


Figure 2. MM Usage Frequency

The MM platform forms an integral part of about 96.7% of the respondents' financial transactions on a daily and weekly basis. This inadvertently could provide SE attackers a repeated opportunity to harvest users PII i.e., full names and corresponding phone numbers. This opportunity could heighten the likelihood of tailored SE schemes, such as phishing or impersonation attacks.

Awareness & Vulnerability Perception

A study by Lappeman et al. highlights a significant level of digital privacy concern amongst consumers regarding how their PII is handled by chatbots. This concern is heightened by high-profile data breaches incidents such as the Cambridge Analytica-Facebook event, which in turn has raised awareness about data privacy issues. Their research found that, privacy concerns negatively impact users' willingness to disclose PII to chatbots. This concern indicates that, even if consumers are aware of the benefits of using chatbots, their apprehensions about privacy can hinder their engagement [28]. This assertion by Lappeman et al collaborates one of the key findings of this paper i.e. user awareness of inherent risks in MM transaction.



Do you think the exposure of your full name and phone number during mobile money transactions make you more vulnerable to scams or attacks?

60 responses

Figure 3. Vulnerability Perception

A 96.7% respondents awareness regarding PII exposure during MM transaction was recorded. In addition, a 76.7% felt this exposure places them at greater risk as in Figure 3 above. This perceived risk aligns with the paper's objective of theorising an expanded SE attack surface in MM platforms.

Social Engineering Risks

Table 2. SE Risk

Question ID	**Question Text**	**Response Option-1**	**Response Option-2**	**Response Option-3**
Q10	Have you ever experienced any suspicious behaviour or phishing attempts after making a mobile money transaction, where the attacker referenced your name or phone number?	Yes [48.3%]	No [51.7%]	
Q11	Would you feel safer if your mobile money transactions did not expose your full name and phone number to the recipient?	Yes [38.3%]	No [53.3%]	Maybe [45%]
Q12	Have you ever reported a fraudulent mobile money transaction or social engineering attempt to the service provider?	Yes [38.3%]	No [16.7%]	I didn't know I could report it [8.3%]
Q13	Do you think mobile money providers should do more to protect users	Yes, a lot more [81.7%]	Yes, somewhat [13.3%]	No, they are doing enough [5%]

	from scams and social engineering attacks?			
Q14	Do you think that there is enough public awareness about the risks of social engineering and scams related to mobile money?	Yes [28.3]	No [65%]	Maybe [6.7%]

This section focuses on SE risks per user experience in connection with the MM platform. The analysis is based on the responses in Table 2 above. Quite significantly, almost half (48.3%) of the respondents reported experiencing suspicious behaviour or phishing attempts where their PII i.e., name or phone number, was referenced. This implies that, a substantial proportion of users have already faced potential SE attempts after MM transaction. A slight majority i.e., 51.7% reported no such experience as of yet. But, the values recorded for Q10 “Yes” and “No” responses were almost equally split suggesting the pervasiveness of the risk but not universally recognised.

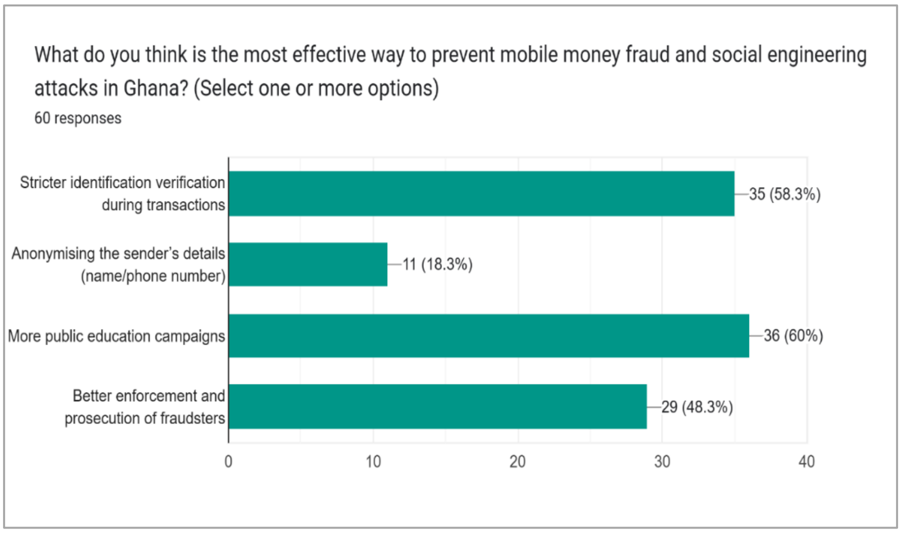
With respect to Q11, 38.3% explicitly felt that, masking their PII during MM transactions would make them safer but a majority i.e., 53.3% did not share this sentiment. In addition, 45% were uncertain; this indicates a divergence in user perceptions of the link between PII exposure and SE risks. Per the response data, many users might not be in the position to fully appreciate the implications of PII exposure in enabling social engineering attacks.

Q12: A notable 38.3% of the respondents has once made an attempt at reporting fraudulent SE attempts. This demonstrates that, many users actively come to face and somewhat recognise such threats. However, the 8.3% who were unaware they could report such incidents points to lack of awareness about reporting channels. The 16.7% who did not attempt at making any report might point to doubt about the effectiveness of embarking on such exercise.

Q13: Overwhelmingly, 81.7% of the respondents felt owners of MM platforms should do more at protecting users. This assertion was supported by an additional 13.3% expressing a moderate agreement. Notably, only 5% were of the believe that, the existing measures in place are adequate. This highlights an obvious dissatisfaction with the existing security provisions. The responses further underscore a strong demand for improved security measures, such as masking PII during MM transactions. This aligns with the study's objective of minimising the attack surface of the current system's design. The response also reflects users' awareness of the need for systemic solutions to address vulnerabilities in the MM platforms.

Q14: Majority of the respondents i.e., 65% were of the opinion that, there is insufficient public awareness about the risks associated with SE and scams regarding the MM domain. In contrast, 28.3% felt there is enough awareness. However, a 6.7% expressed uncertainty about the effectiveness of current awareness efforts. The findings highlight a significant gap in public education and awareness campaigns, which is a very important knowledge users must have to help them recognise and prevent SE attacks. Furthermore, the role of MM providers, regulators, and policymakers at designing and implementing effective awareness campaigns to bridge this knowledge gap is called into question. This paper posits that, the lack of awareness contributes to the vulnerabilities created by PII exposure, making users easy targets for SE attacks.

This section’s responses point to a substantial incidence of PII related threats and a widely perception that existing protection measures in the MM platform domain are inadequate. This calls for a systemic change which is strongly supported by the findings and the paper’s hypothesis that MM transaction processes as currently designed increases the attack surface for social engineering. There was also a call for public awareness about SE risk that brings to the fore a needed drive for user education as a central component of the solutions of the identified risks. A multiple response question in Figure 4 below reinforces the emphasis on the importance of public education campaigns. This garnered the highest percentage of 60% which underscores the recognition awareness plays in equipping users to appreciate SE schemes.



What do you think is the most effective way to prevent mobile money fraud and social engineering attacks in Ghana? (Select one or more options)

60 responses

Figure 4. User-Perceived Solutions

The spread of the responses, as captured in Figure 4 above, suggest that no single solution could effectively deal with the problem but rather a solution that encompasses stricter verification, education, enforcement, and possibly anonymisation. In contrast, respondents lower prioritised data anonymisation which this paper considers as one of the key solutions to resolving the PII exposure problem. This implies that, respondents either undervalued the role of data anonymisation at reducing the SE attacks or are less informed about its potential impact. Anonymisation techniques, such as the dynamic anonymity privacy-preserving model, help to reduce information loss and can potentially improve data usability by processing data across multiple granularity spaces and applying differential privacy principles [29]. In the context of cloud services, as demonstrated by the Clustering Permutation for data Anonymisation (CPA), anonymisation ensures that data privacy is maintained without altering the context of the data, thus supporting compliance with privacy laws [30].

Conclusion

The outcome of this paper reaffirms a critical vulnerability within Ghana’s MM ecosystem. The MM platform’s design exposes users’ PII, specifically their full names and phone numbers thereby creating a fertile ground for SE attacks. By making such data readily accessible during MM transactions, the MM platforms inadvertently expand the attack surface for fraudsters — aligning strongly with the hypothesis that, MM platforms by their current design, heighten the attack surface for SE.

The major outcomes of the study revealed a complex interplay of awareness, risk perception, and security gaps. While most users recognise the visibility of their PII and its potential for misuse, a troubling disconnect persists between this awareness and their trust in the platform's safety. Alarmingly, nearly half of the respondents reported being targeted by phishing attempts referencing their PII after MM transaction, and a majority acknowledged the need for greater protections. Yet, despite these risks, many remain quite hesitant about the adoption of certain preventative measures, such as anonymising sender details; an indication of both cultural trust in the system and insufficient understanding of how social engineering operates.

Yet, the deeper question remains; how far could technological and educational interventions go in mitigating risks that are embedded within the very structure of MM platforms? Are MM platform owners thus willing to fundamentally reengineer their systems to prioritise user anonymity without compromising transparency and convenience?

Conflict of Interest

I, Daniel Adjei Odai, hereby declare that, there are no conflicts of interest regarding this research work.

Acknowledgement

I express my profound gratitude to the questionnaire respondents and also to my wife for her valuable support and encouragement

References

[1]. A. Amoah, K. Korle, and R. K. Asiama, 2020,"Mobile money as a financial inclusion instrument: what are the determinants?". *International journal of social economics*, vol. 47, no. 10, pp. 1283-1297

[2]. I. Akomea-Frimpong, C. Andoh, A. Akomea-Frimpong, and Y. Dwomoh-Okudzeto,2019,"Control of fraud on mobile money services in Ghana: an exploratory study,2019".*Journal of Money Laundering Control*, vol. 22, no. 2, pp. 300-317

[3]. M. R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, and N. Kaabouch,2020,"Social Engineering Attacks a Reconnaissance Synthesis Analysis".In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), vol. IEEE, pp. 0843-0848

[4]. M. Sillanpää, and J. Hautamäki, 2020,"Social engineering intrusion: A case study".In Proceedings of the 11th *International Conference on Advances in Information Technology.*

[5]. S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld, and A. Laszka, 2022,"Survey and taxonomy of adversarial reconnaissance techniques".*ACM Computing Surveys*, vol. 55, no. 6, pp. 1-38

[6]. I. Makhdoom, M. Abolhasan, J. Lipman, N. Shariati, D. Franklin and M. Piccardi, 2024,"Securing Personally Identifiable Information: A Survey of SOTA Techniques, and a Way Forward". IEEE

[7]. J. A. Jamin, M. S. Noor, N. Rosli, and A. Shukry, 2019,"Privacy concern of personal Information in the ict usage, internet and social media perspective".*Malaysian E Commerce Journal*, vol. 3, pp. 15-17

[8]. H. Nissenbaum, 2011,"Privacy in context: Technology, policy, and the integrity of social life,2011".*Journal of Information Policy*, vol. 1, pp. 149-151

[9]. R. N. Zaeem, and K. S. Barber, 2020,"The effect of the GDPR on privacy policies: Recent progress and future promise,2020".ACM *Transactions on Management Information Systems (TMIS)*, vol. 12, no. 1, pp. 1-20

[10]. R. Apau, and F. N. Koranteng, 2020,"An overview of the digital forensic investigation infrastructure of Ghana".*Science International: Synergy*, vol. 2, pp. 299-309

[11]. A. Narayanan, and V. Shmatikov, 2008,"Robust de-anonymization of large sparse datasets".*In 2008 IEEE Symposium on Security and Privacy* (sp 2008), pp. 111-125

[12]. M. Mitra, and S. Roy, 2018,"Identification and Processing of PII Data, Applying Deep Learning Models With Improved Accuracy and Efficiency".*Journal of Data Acquisition and Processing,* vol. 33, no. 6, p. 1337

[13]. Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, 2023,"A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions".*Electronics*, vol. 12, no. 6, p. 1333

[14]. K. Krombholz, H. Hobel, M. Huber, and E. Weippl,2015,"Advanced Social Engineering Attacks".*Journal of Information Security and applications*, vol. 22, pp. 113-122

[15]. G. Iachello. and J. Hong, 2007,"End-user privacy in human–computer interaction".*Foundations and Trends® in Human–Computer Interaction,* vol. 1, no. 1, pp. 1-137

[16]. P. Burda, L. Allodi, and N. Zannone, 2024,"Cognition in social engineering empirical research: a systematic literature review". *ACM Transactions on Computer-Human Interaction*, vol. 31, no. 2, pp. 1-55

[17]. FBI, 2023,"Federal Bureau of Investigation".Internet Crime Complaint Center (IC3) Annual Report 2023, https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

[18]. V. Bhavsar, A. Kadlak, and S. Sharma, 2018,"Study on phishing attacks".*International Journal of Computer Applications,* vol. 182, no. 33, pp. 27-29

[19]. H. Shahbaznezhad, F. Kolini, and M. Rashidirad, 2021,"Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?".*Journal of Computer Information Systems*, vol. 61, no. 6, pp. 539-550

[20]. M. Zaeifi, F. Kalantari, A. Oest, Z. Sun, G. J. Ahn, Y. Shoshitaishvili, and A. Doupé, 2024,"Nothing Personal: Understanding the Spread and Use of Personally Identifiable Information in the Financial Ecosystem".*In Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy*, pp. 55-65

[21]. K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, and E. Bursztein, 2017,"Data breaches, phishing, or malware? Understanding the risks of stolen credentials".In Proceedings of the 2017 *ACM SIGSAC conference on computer and communications security,* pp. 1421-1434

[22]. A. Yunoose, A. R. Varghese, R. Anagha, A. Prakash, and D. Babu, 2022,"Phishing".*International Journal of Engineering Technology and Management Sciences,* vol. 5, no. 6, pp. 574-579

[23]. C. Andrade, 2020,"The limitations of online surveys".*Indian journal of psychological medicine,* vol. 42, no. 6, pp. 575-576

[24]. NCA, 2024,"Shaping the Future – The NCA's Achievements".National Communications Authority, https://nca.org.gh/wp-content/uploads/2024/12/NCAs-Achievements-1.pdf

[25]. B. Walther, S. Hossin, J. Townend, N. Abernethy, D. Parker, and D. Jeffries, 2021,"Comparison of electronic data capture (EDC) with the standard data capture method for clinical trial data".*PloS one,* vol. 6, no. 9, p. e25348

[26]. A. Travis, 2024,"Digital Literacy and Media Consumption among Different Age Groups," *Journal of Communications*

[27]. A. Antonio, and D. Tuffley, 2015,"Bridging the age-based digital divide".*International Journal of Digital Literacy and Digital Competence (IJDLDC),* vol. 6, no. 3, pp. 1-15

[28]. J. Lappeman, S. Marlie, T. Johnson, and S. Poggenpoel, 2022,"Trust and digital privacy: willingness to disclose personal information to banking chatbot services".*Journal of Financial Services Marketing,* vol. 28, no. 2, p. 337

[29]. J. Qian, M. Zheng, Y. Yu, C. Zhou, and D. Miao, 2025,"A dynamic anonymization privacy-preserving model based on hierarchical sequential three-way decisions".Information Sciences, vol. 121316, p. 686

[30]. M. Silveira, D. Santos, M. Souza, D. Silva, M. Mesquita, J. Neto, and R. L. Gome, 2023,"An Anonymization Service for Privacy in Data Mining".In Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing, pp. 214-219