Mobile Money Phishing Cybercrimes: Vulnerabilities, Taxonomies, Characterization from an Investigation in Cameroon

Alima Nzeket Njoya[1,2], Franklin Tchakounté[1,2,3](✉), Marcellin Atemkeng[3], Kalum Priyanath Udagepola[4], and Didier Bassolé[5]

[1] Department of Mathematics and Computer Science, Faculty of Science, University of Ngaoundere, Ngaoundere, Cameroon
[2] Cybersecurity With Computational and Artificial Intelligence Group (CyComAI), Ngaoundere, Cameroon
{j.ntsama,f.tchakounte}@cycomai.com
[3] Department of Mathematics, Rhodes University, Grahamstown 6140, South Africa
m.atemkeng@ru.ac.za
[4] Department of Information and Computing Sciences, Scientific Research Development Institute of Technology, Loganlea, Australia
kalumu@srdita.com.au
[5] Laboratory of Mathematics and Computer Science, University of Joseph Ki-Zerbo, Ouagadougou, Burkina Faso

Abstract. Mobile Money (MM) technologies are popular in developing countries where people are unbanked, and they are exploited as means of financial transactions in the economy. Sophisticated cyber-phishing techniques successfully target MM accounts. Related countermeasures are rare and the existing ones are so technical that people without minimal knowledge cannot be helped. Making the knowledge around cybercrime facts is therefore relevant since it provides a good basis for further technical research. In this vein, this paper dissects phishing cybercrime strategies observed within the Cameroonian cyberspace. We provide identified vulnerabilities, process design of generic MM attack, taxonomies of attacks, and classification of the latter based on criteria. Findings about commonalities and dissimilarities reveal two aspects to really consider when designing solutions: emotion and interactions.

Keywords: Mobile money · phishing · vulnerabilities · taxonomies · emotions · interactions · cybercrimes · cameroon

1 Introduction

Mobile payment or Mobile Money (MM) allows people to accumulate, send and receive money using their mobile phone without having a bank account [1]. This technology is widely and effectively used in many countries where populations are still unbanked

R. A. Saeed et al. (Eds.): AFRICOMM 2022, LNICST 499, pp. 430–445, 2023.
https://doi.org/10.1007/978-3-031-34896-9_26

and where banking services are unavailable and/or in crisis, such as during the Covid-19 pandemic, access to societal facilities (transport, trade, hospital, …) are limited [1]. According to the World Bank, this technology is a vector of economic growth and therefore of the objectives of sustainable development in developing countries [2]. In sub-Saharan Africa, the world's most popular mobile payment region, 64.15% of global transaction volume was recorded in 2019, followed by 19.7% growth in 2020 [3]. In Cameroon, it generated 17.5% of the gross domestic product (GDP) in 2017 [4–6] and made it possible to control the risks associated with savings operations in households [4, 7, 8]. However, the popularity of Mobile Money is growing with the attractiveness of cyber-scammers who are experts in stealing money and sensitive information. Indeed, they use social engineering techniques such as phishing [9] to manipulate victims and get them to unknowingly disclose their confidential data [10]. Based on the psychology of the user, phishing caused the Cameroonian economy to lose 12.2 billion in 2021, i.e., double that in 2019 [12]. It is one of the most criminal to which effective user-centered solutions must be provided [9].

Many works exist to fight against this scourge. While some more technical exploit emerging technologies such as artificial intelligence [12–17], others which require minimal knowledge in ICT [18, 19], are intended for education and awareness of people.

However, the complexities related to the categories of solutions, leave victims open to attack. Which leads us to think that it would be useful to dig into the actual unfolding of the attacks. This could thus contribute to adding new ingredients to the technical solutions and to orient awareness in a more comprehensible way from the point of view of the consumer.

This work provides a characterization layer of Mobile Money cyber-crimes with a particular investigation of mobile network operators (MNO) in Cameroon. More particularly, we contribute to three points.

- First, we provide threats identified and justified within the mobile payment services. We have matched to the security services which are violated such as confidentiality, integrity, availability to name a few.
- Second, we design a four-step process flow to represent general mobile money cybercrimes. Each step has been elucidated in relation to vulnerabilities in the first contribution.

Third, we provide a taxonomy of MM attacks based on observations. They have been classified based on defined criteria and findings constitute solid knowledge of commonalities and dissimilarities to consider when designing solutions.

The remainder of the paper is structured as follows. Related works are presented in Sect. 2. Section 3 describes some background on mobile money motivations and social engineering aspects. Section 4 explains how we proceed with acquisition of cybercrimes. Section 5 describes the vulnerabilities observed in the mobile payment systems. The process flow of generic MM attack is described in Sect. 6. Section 7 shows how taxonomies of attacks are created. Section 8 concerns the classification of these taxonomies in classes based on specific criteria. In the same section, findings are explained and key aspects for solutions are discussed. The document is ended with a conclusion and perspectives are mentioned.

2 Related Works

Phishing detection is a crowded domain of research. However, specific phishing such as the one in mobile money remains not deeply visited. In the next, the main trends of approaches are described.

A cybercrime is an activity which can be identified due to some features identified during the process. So, researchers look inside vectors such as email, phone calls and URLs to determine whether a set of fields with specific values are used during the attack. As a human, this exercise becomes complicated when there are a lot of things – a hundred for example - to discover. What authors do is to be assisted with artificial intelligence to automate the process. For instance, Gandotra and Gupta [12] exploit machine learning algorithms on 4898 phishing and 6157 normal webpages, each page structured in 30 features with a high phishing detection accuracy. Extensive surveys are provided for such solutions in terms of using deep learning [13, 14] and machine learning [15]. Emergent technologies are also targets for phishing. Some other authors investigate phishing arising in blockchains. MP-GCN [16] is designed to identify phishing in Ethereum networks. After modelling as a graph, authors adopt feature engineering and dimensionality reduction to give a graph convolution network. Authors in [17] use ensemble learning on collected Ethereum transactions, which are structured as labelled graphs.

Educational games are designed to improve phishing reconnaissance to the players. In this vein, Panga et al. propose an educational mobile game for teenagers in Tanzania [18]. Likewise, a game-based training has been built and contextually evaluated in [19]. Moreover, telecom operators and media owners vehiculate sensitization through media channels.

As targeted in these works, detection performance is not the concern in this study. We are not looking to have more complex solutions which could not be used by simple people. But we are interested in understanding in depth and characterizing the processes of cybercrimes. In so doing, consumers will be more aware of the cybercrime intentions and cybersecurity professionals will be more. We believe that if we provide people with dissected components and justifications, their comprehension will be more improved and therefore mistrust elevated. This work is therefore complementary to sensibilization improvements.

3 Background

In this section, some background concerning mobile money and social engineering are presented.

Ondrus and Pigneur [20] define mobile payment as a transaction of monetary value between two parties, through a mobile device capable of securely processing a financial transaction over a wireless/telecom network. According to Mbiti and Weil [21], mobile payment is a service offered by a mobile telephone network, allowing users to deposit funds in their personal account, to make funds transfers by short messages, to make withdrawals, to pay bills, to name but a few.

In general, a mobile payment system is made up of the following entities [22]: (i) Customer (C) is anyone who looks for services from the merchant such as the transfer

of money and the payment of invoices to name a few. (ii) Merchant (M) providing the service. (iii) Acquirer (A) is the institution responsible to manage the merchant's account and the verification of the payment instrument filed. (iv) Issuer (I) is the financial institution that manages the customer's account and provides electronic payment instruments to be used by the customer. (v) Payment gateway (PG) is that entity, intermediary between the buyer and the issuer. In general, issuers are mobile network operators (MNO).

According to Bahri-Domon [23], mobile payment was initiated in Cameroon for the very first time in 2011. In his study, the author presents four important platforms for mobile money services in Cameroon, namely MTN Mobile Money, Orange Money, Express Union Mobile Money and Nexttel. Although banking institutions increasingly turn to mobile money services, MTN and Orange remain the two MNO dominating this sector. Together they have 5.4 million registered users [24]. Hence, cybercrimes targeting these two issuers are concerned within this work.

This economic sector attracts malicious people who multiply social engineering (SE) strategies. Social engineering is helpful to them because they need to lure, to manipulate the psychology of their victims. The final aim is in fact to put the victim in a situation of confidence where any fake request will be considered and realized. The popular SE vector is email from where fake content, links and attachment are embedded. Since we are talking about unbanked people who hardly have emailing services, phishing related to mobile money is considered and therefore cybercrimes through mobile phones. In the following, the process flow of mobile money cybercrime is designed.

4 Collection of Cybercrimes

This study is concerned with mobile money cybercrimes through mobile phones. This concerns cybercrimes which target mobile money accounts. For that, we have investigated situations of cybercrimes which happened to people in the country, in our environment as well as those we met in person. The approach was to investigate social media spheres such as Facebook, Whatsapp and Twitter, complaints about MM phishing. Also, we enriched the knowledge with advertisements or sensitizing artifacts released in media channels such as newspapers, television and radio. With the advantage of being expert in the area, it was straightforward to discern interesting requirements from stories. Since it has been impossible to directly have information from telecom operators due to confidentiality, we were obliged to informally be on permanent watch for phishing stories. Apart from scrutinizing media and social media, we sometimes proceeded to genuine and informal questions to people who seemed to have already been exposed. In case, similar stories we discarded duplicates. We mean by discarding to consider two similar phishing stories in the same category.

5 Threats Found in MNO

Here, we describe certain threats discovered during the investigation concerning money transactions. But before, the transaction process should be presented. The prior requirement is that the customer creates a MM wallet exploited for withdrawals and deposit transactions. For that, subscribers must be identified using valid identity documents in conformance with laws [25]. Then a confidential code or Personal Identification Number (PIN) is created by the user to secure the wallet. A country-specific code called Unstructured Supplementary Service Data (USSD) identifies the service and must be dialed to start the process. For instance, #150# refers to money transfer in Orange and *126# in MTN. Once the user has dialed the code, steps are guided until he specifies the amount and the receiver number [26] the name of the receiver asking to confirm the operation. Indeed, the process requires entering a PIN code. All those steps can be equivalent to a sequence of codes. Table 1 illustrates six main threats referring to (ti) with their description and violated security services.

Table 1. Threats

Threat ID	Threat	Description	Service violated
t_1	Disclosure of name	The attacker can simulate the intention to make a transfer just to capture the name of people	Confidentiality
t_2	Sequence of code incomprehension	Each MNO provides its way of accessing services through sequences of codes starting with the USSD. For a simple user, the semantic of that is unknown. Therefore, he/she can be misleading to put a sensitive value somewhere to leak information	Integrity and availability
t_3	Presence of unidentified SIM card	Until now, there are sellers of SIM Cards of obsolete pre-identified cards or even unidentified constraints. Cybercrimes are catalyzed with these bad people who maintain the black market of fake SIM cards. People are therefore able to repudiate a bad action. Really controlling this means to identify these markets [25, 27]	Authentication and non-repudiation

(*continued*)

Table 1. (*continued*)

Threat ID	Threat	Description	Service violated
t_4	Non-compliance during registration	This threat is about (i) using fake ID cards (ii) exploitation of lost identity cards and (iii) usurpation of identity [28] It seems difficult for MNO to control this aspect since there are no centralized and connected systems of identifications. Moreover, human controllers during registration are not so efficient when there are a lot of customers to serve. These three cases give authorization to do bad actions due to fake credentials and therefore, they will be able to repudiate some cybercrime	Confidentiality, Authentication, Authorization and non-repudiation
t_5	Phone and pocket stolen	People used to store PIN codes in the phone or in their pockets. In case they are lost, people will obviously steal information	Confidentiality, Integrity, Availability
t_6	Initiation of transaction	We observed that you can initiate the transaction on behalf of someone else. This relies on T_1 helpful to get some credentials. Indeed, you couldn't follow without the PIN and the concerned will be triggered as well	Confidentiality

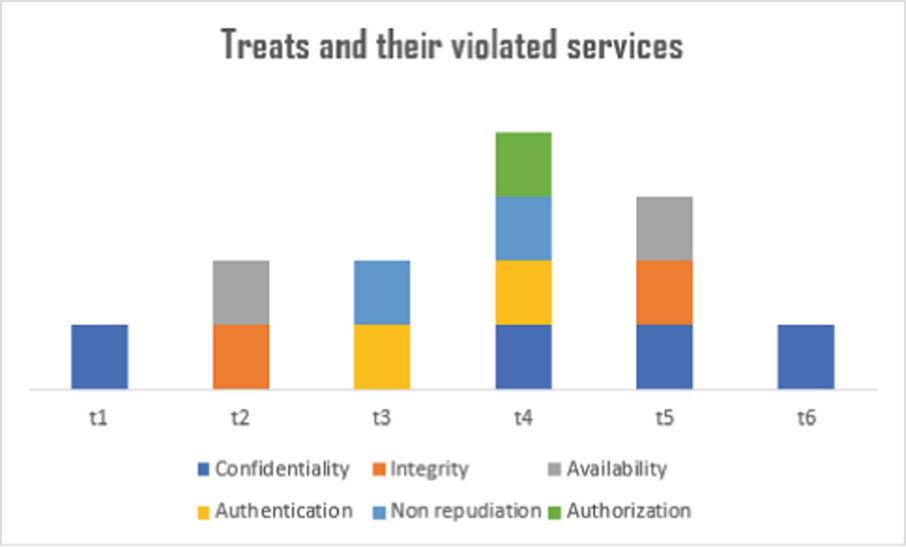

Fig. 1. Diagram of treats and violated services

Figure 1 synthetizes the content of Table 1.

As we can see in this figure, only one security service (confidentiality) has been violated concerning threats t_1 and t_6. Threats t_2 and t_3 have both violated two security services. Integrity and availability for threat t_2; authentication and non-repudiation for threat t_3. However, regarding threat t_5, we observe that there are up to three security services violated such as confidentiality, integrity and availability. Finally, with threat t_4, all the security services have been violated. This means that; threats t_4 and t_5 are the most dangerous in the attack during the process of transaction money.

6 Mobile Money Cybercrime Process Flow

Based on the cybercrimes previously characterized, the process flow illustrated in Fig. 2 has been designed to represent mobile money cybercrimes. It includes four steps. First, an attacker investigates the alleged victim in order to gather some basic information needed to carry out his attack. Second, the attacker uses this information to contact the victim and coax him by playing on his emotions. Third, an attack is launched without the victim suspecting anything and obtains the victim's personal code or a deposit of money made by the victim. Fourth, whatever the attacker has obtained, this stage is to disappear without leaving any traces.

Figure 3 gives another representation of the process flow.

As we can see in this figure, during the stages of manipulation and execution of the attack, the attacker exploits many more threats than during the other stages (gathering information and planning the end of the attack). This fact means that manipulation and execution of the attack include more decisive and complex steps to complete than in the other stages. Indeed, the attacker is likely to win if he succeeds in manipulating the

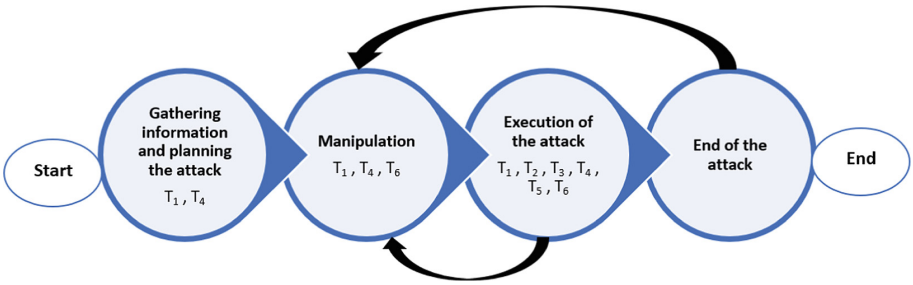

Fig. 2. Process flow

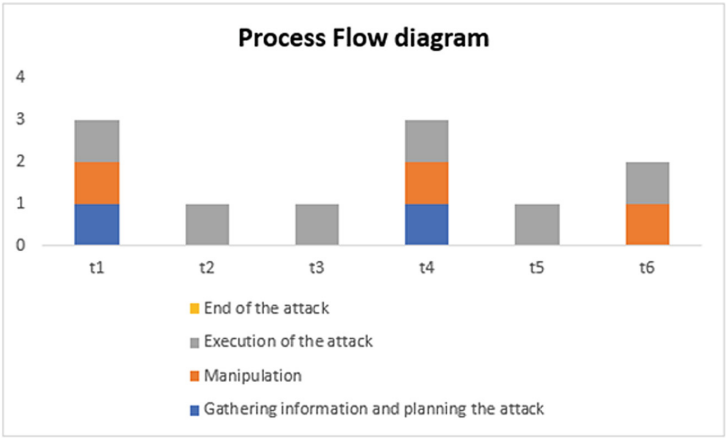

Fig. 3. Process flow diagram

victim. The attacker also fails if the technique is not as smarter as the potential victim could detect.

Gathering Information and Planning the Attack: The attacker defines his target which can be an individual or an organization and collects details about them by physically visiting them, monitoring them or collecting information through social networks, the Web, physical media, relatives and friends. He thus chooses a feasible means of communication to launch the phishing attack and get in touch with the victim. This means it can be a call or an SMS. Once this attack technique is selected, the attacker can then proceed to the next stage which is manipulation. In this stage, the target is even knowingly selected or unknowingly selected, both cases through mobile phone numbers. In the first case, the attacker could have been investigating the victim on social media such as Facebook for quite long, the time to collect enough information and to learn weaknesses. Based on his/her interest and seen people divulging their phone number and daily life. For instance, a person who had a promotion can be susceptible and of interest or a person with a high standing status in society. As information such as the phone number are easily provided on the Web, the attacker will just have to retrieve the name and/or surname through threat t_1 described in Table 1. Threat t_4 is also a source

exploitable by the attacker in this stage, since they make calls with fake identities to get some personal information on the target.

Manipulation: The attacker contacts the victim by means of an SMS or a call. The goal of making contact is to develop a relationship of trust with the victim, a relationship that might lead them to see the attacker as someone familiar and whom they could trust or need. to communicate. To build this relationship and hook the victim, the attacker makes the victim confident and prepares the ground for his attack. One of the keys for the attacker is the use of the exact name taken due to t1 and t_4. During this phase, the attacker asks a series of questions or holds a conversation that motivates the target to follow the path they want. He begins by asking his target very neutral questions to which the answers will most likely be yes or no, then he moves on to a few open questions, accompanied by a few closed questions while directing the victim towards the final goal which is the scam. With good communication and psychological skills, he manipulates the victim's emotions by adapting the conversation to his environment and situation. He listens for example to the tone of the victim's voice; he launches a funny word and reassures himself that the victim will laugh or be amazed. It can also create emergency situations related to the victim's experience. For example, he can simulate crying to get the victim to panic and act as he pleases. Threat t_6 can occasion successful manipulation.

Execution of the Attack: In this phase, the attacker is ready to launch his attack because through a certain number of emotions activated in the victim during the manipulation phase, he is sure to have put him in confidence. He therefore creates a scenario in which he will lead the victim to take an action or perform an action to activate this attack phase (this may be the fact of disclosing personal information about him or giving his PIN code without realizing or making a deposit to the attacker). According to Laird and Oatley [29], a well-crafted script creates an atmosphere in which the victim feels comfortable disclosing information that they would not normally do. Social engineers design different scenarios in different attacks. And each scenario aims to activate specific emotions in the victim, emotions that can be exploited by the scammer to succeed in the attack. A good scenario therefore manipulates emotions to establish a situation of trust in the victim and lead him to do what the attacker wants. Developing the relationship and executing the attack therefore involves the victim directly disclosing sensitive information about themselves or doing things they normally would not do. It is in these stages that the victim's emotions are aroused, influenced and manipulated. A social engineer is very adept psychologically, socially, technically and emotionally as he uses pretense, tricks and influences to control and manipulate the emotions of the victim and drive him towards his goal [29]. The attack is most often conducted with a series of calls and different people involved in the process to really lure the victim. The case studies will show all the details. This stage is favorized by all the threats in Table 1. Here, the attacker can restart manipulation if it seems the victim has learned the tips.

End of the Attack: The end of the attack is marked by the fact that the victim has transferred the content from the wallet to the attacker or has mistakenly provided a PIN code. Therefore, the attacker empties the victim's account. In case the victim discovers the fraud, the action which follows is to cancel the phone calls and the ongoing transfer if it was about to be launched. What allows awake victims to detect are generally to

take advice from relatives. Some experiences may reveal similar strategies. So once the attacker succeeds or fails in executing his attack, he can simply walk away, cover his tracks as much as possible, and prepare for the next attack. The information collected and the scenario used during this attack as well as the skills acquired during the attack are updated to move on to the next attack. The attacker may have to reiterate other manipulation techniques if he feels that the victim is suspecting (see the back arrow). For example, involving a fake relative of the victim during the conversation.

7 Taxonomizing Cybercrimes

In this section, we have compiled and relooked MM phishing stories in seven taxonomies. These taxonomies are essentially obtained based on observations coupled with expertise and some literature. Some statements are supported by literature (Fig. 4).

Fig. 4. Taxonomies

MM Identity Theft (T_1): This is a form of mobile money crime committed by a friend, relative or fraudster who steals owners' financial information such as PIN to complete transactions. According to Bosamia [30], when a customer's mobile phone is stolen, attackers use all the sensitive data stored on it, including the PIN code, and control the device. The mobile money PIN code stored on the mobile phone allows them to access the MoMo account thus enabling them to perform fraudulent transactions.

MM Authentication Attack (T_2): It is a mobile money crime where attackers target and attempt to exploit the mobile money authentication process by applying brute force attack or weak PIN code attack. This is consistent with the findings of Mtaho [31], who found that attackers use many means to gain access to users' accounts and take advantage of weak PIN reset procedures, making it easy to guess, smudge, or spying. This result is also consistent with the study conducted by Bosamia [30], which reported that most mobile money systems are not adequately protected, giving cyber fraudsters the opportunity to apply reverse engineering (RSE) to attack hard-coded passwords or PINs, encryption keys and steal customers' money.

MM Phishing Attack (T_3): This is a form of mobile money crime where fraudsters pose as employees of the mobile money service provider by calling or texting users to reveal their data, including a PIN code for an update. This is in line with observations by Bosamie [32], who also found that fraudsters carry out sophisticated attacks by either

emailing, texting, texting or calling mobile money users to disclose their personal and financial information.

MM Vishing Attack (T_4): This is a form of mobile money fraud in which fraudsters use voice calls to trick users and mobile wallet agents into revealing their personal financial information such as a PIN. This confirms the findings of previous studies by Saxena et al. [33], Maseno et al. [34] who observed that attackers use anonymous phone calls or fake promotions to trick users into disclosing their PINs or other sensitive personal information which is then used to steal their mobile money accounts.

MM Smishing Attack (T_5): This is a form of mobile money fraud where fraudsters send delirious emotional text messages to trick users and mobile money agents into revealing their mobile money account information, including the PIN code. This result is described in previous studies by Maseno et al. [34], where fraudsters send fake text messages using their mobile phones to mobile money users and mobile money agents and then take them through different stages, which later results in the money transfer from their account to the fraudsters' account. It is also consistent with studies by Akomea-Frimpong et al. [35], Gilman and Joyce [37], Lonie [37] who reported that fraudsters posing as employees of mobile service providers send fake text messages to customers that they have won a promotional prize, and for them to claim the price to be paid for sending money to the fraudster's number.

MM Agent Fraud (T_6): Mobile money agents also experience fraud from attackers and users, thereby threatening the security of the platform. This finding is consistent with work by Buku and Mazer [37], Lonie [37], in which they found that common acts of fraud experienced by agents include loss of flow in the agent's account resulting from unauthorized use, misuse of PINs, and a fraudster impersonating an agent to gain unauthorized access to the agent's checking account.

MM USSD Vulnerabilities (T_7): The greatest risk of the USSD system is that information transported in the communication channel is not encrypted, thus making the USSD data vulnerable to attack [37]. This is consistent with Mtaho's submission [31] who noted that during the verification process, the client enters the PIN that goes through the USSD system to the server in plain text; thus, attackers using sniffing software such as Wireshark can intercept it.

8 Classification

Table 2 provides a classification of taxonomies according to six criteria. The first criterion refers to the element exploited to transmit the attack. It can be the SMS in the case where the attacker shapes a false message to deceive the victim. The attacker can also coax the victim through phone calls. The second criterion is the threat facilitating the success of cybercrime. The different threats are already explained in Table 1. The third aspect represents the emotional aspects incited in the victim during the attack. For example, during the call the cybercriminal may want to put the victim in a state of trust with respect to his recommendations. The fourth aspect includes the key elements without which the attack would not be sophisticated. The fifth criteria indicates whether there

were probably a multitude of interactions (multi-stage) for the attack to succeed in convincing the victim or only one interaction (one-stage). The sixth criterion highlights the categories of victims concerned.

Table 2. Classification

Taxonomies	Attack vector	Threat	Emotional aspects from victim	Key elements for succeeded attack	Interaction type	Victims
T_1	Stolen device	t_5	None	Available PIN	None	Consumer
T_2	Malicious attempts	t_6	None	brute force, weak PIN	None	Consumer
T_3	SMS, voice calls	t_3, t_4	Confidence	Identity usurpation	Multi-stage	Consumer, MNO MM Agents
T_4	Voice calls	t_1, t_2, t_3, t_4, t_5, t_6	Confidence	Manipulation tips	Multi-stage	Consumer
T_5	SMS	t_6	Delirious, happy, surprise	Content of SMS	One-stage	Consumer
T_6	Voice calls, Malicious attempts	t_2,t_3,t_6	Confidence	Bad use of code PIN, impersonation	One-stage	MM Agent
T_7	Uncovered channel	Lack of encryption	None	Sniffing	None	Consumer

Figure 5 synthetizes the taxonomies with their threats.

We mentioned above that, MM Vishing attack (T_4) is a form of mobile money fraud in which fraudsters use voice calls to trick users and mobile wallet agents into revealing their personal financial information such as a PIN. As we observe in the Fig. 5., T_4 is the only one kind of attack which exploits all threats which means that MM Vishing attack can be qualified as the most dangerous attack between all the taxonomies we mentioned on the above.

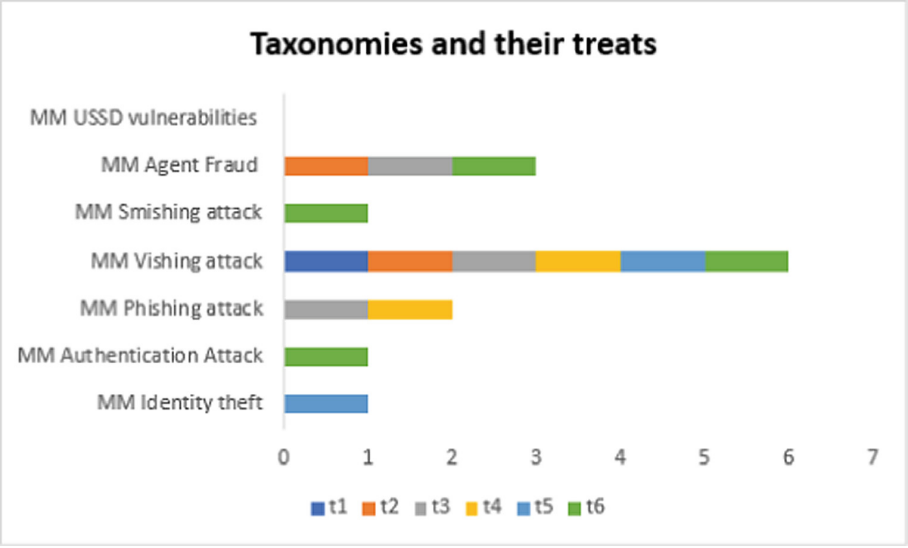

Fig. 5. Taxonomies and their treats

8.1 Findings

Several observations follow from the table. We present them criterion by criterion and then as a whole. Most mobile money attacks are perpetrated through text messages and calls. Indeed, these means easily retain the victims when they are in contact by the manipulated voice and by the written text of the attacker. Threat t_6 comes back more because it is probably in vogue for its ease of deployment. We note that some attacks are technical (T_7) and linked to the issuer's system. Imagine that the target is someone who could be deceived. The victim receives a message asking to consult the balance because of winning a sum of 100,000 CFA.

The immediate consultation makes it possible to validate the transaction which was initiated by the attacker on his account. We also see that the security services targeted are integrity because the electronic wallet is emptied; confidentiality because the attack scenarios require identity theft and services related to non-repudiation since the attacker uses credentials that are not his. To achieve this, it is necessary to trigger emotions of trust in the victim because he must believe in everything that comes from the attacker, emotions of panic through deadlines to be met or through messages of death or delusional events, and pleasant surprises when it comes to winnings that positively impact the victim's life.

It should be noted that during the attacks, these emotions created aim to make the victim a slave to the attacker. Criterion 4 reveals that the PIN code is the key element sought by attackers during their processes. Added to this are identity theft tricks to reinforce emotions. Through criteria 5, we note that the attacker will in some cases be required to repeat the interactions, possibly with different accomplices, to prevent the victim from noticing. The victims most affected are individuals with an electronic wallet, but they can also be agents of the mobile payment service. This shows that this type of cybercrime can also affect expert people.

Typically, the attacker seeks the PIN from the victim or through threats related to theft and loss activities. The first case is the most popular that requires emotional manipulation.

8.2 What Aspects Would be Interesting for Solutions Against MM Phishing

Table 2 reveals two things to consider. The first concerns the interactions between the victim and the attacker. We believe that you must control what happens there in time and be able to represent it in the form of states-transitions. Thus, the valued connections will likely bring out characteristics that indicate similarities in attacks. The second thing concerns emotions. Emotion is an important element that can be obtained from the human voice through very specific features. Researchers can try to characterize an MM phishing interaction based on the emotions of the two interlocutors. Thus, we believe that we will be able to see how the emotion of the victim adapts according to that of the cybercriminal. The emotions that emerge may be able to characterize a situation of deception or manipulation. These two aspects can be manipulated by artificial intelligence techniques such as deep learning, computer vision or even reinforcement learning.

9 Conclusion et Perspectives

This study concerned the investigation of cybercrimes directed in mobile payment. It was conducted in Cameroon and made it possible to identify the threats related to the payment system, to characterize an attack by mobile payment in general, to create taxonomies of attacks according to the scenarios observed through our observations and finally to create a classification of these taxonomies according to criteria. A discussion was able to highlight the key elements that the protectors can consider in the implementation of possible solutions. This work provides a good basis for understanding these kinds of attacks that plague countries where the population is unbanked. As a perspective, MM attack strategies in other countries will be investigated in order to enrich current knowledge.

References

1. Aker, J.: Using mobile money to help the poor in developing countries. The Fletcher School, Tufts University. https://econofact.org/using-mobile-money-to-help-the-poor-in-developing-countries. Accessed 01 Aug 2022
2. Banque mondiale, Rapport de la Banque mondiale : les transactions électroniques sont d'une importance vitale pour la croissance économique. https://www.banquemond-iale.org/fr/news/press-release/2014/08/28/world-bank-report-digital-payments-economic-growth. Accessed 01 Aug 2022
3. Agenceecofin, l'Afrique Subsaharienne et le mobile money. https://www.agenceeco-fin.com/monetique/0804-75539-l-afrique-subsaharienne-a-genere-64-15-des-transactions-mondiales-par-mobile-money-en-2019. Accessed 01 Aug 2022
4. Finmark. FinScope Consumer Survey Highlights Cameroon 2017. Finmark Trust: Johannesburg, South Africa (2017). https://finmark.org.za/system/docu-ments/files/000/000/220/original/Cameroon-pocket-guide_English.pdf?1601984244. Accessed 01 Aug 2022

5. Andzongo, S.: Cameroon: MobileMoney Transactions Surged to FCFA3500bn in 2017. Investiraucameroun.com.https://www.businessincameroon.com/finance/3108-8300-cameroon-mobile-money-transactions-surged-to-cfa3-500bn-in-2017. Accessed 01 Aug 2022
6. Tengeh, R.K., Gahapa Talom, F.S.: Mobile money as a sustainable alternative for SMEs in less developed financial markets. J. Open Innov. Technol. Mark. Complex **6**, 163 (2020). https://doi.org/10.3390/joitmc6040163
7. Amponsah, E.O.: The advantages and disadvantages of mobile money on the profitability of the ghanaian banking industry. Texila Int. J. Manag. **4**, 1–8 (2018)
8. Must, B., Ludewig, K.: Mobile money: cell phone banking in developing countries. Policy Matters J. **7**, 27–33 (2010)
9. Jai, A.K., Gupta, B.B.: A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterp. Inf. Syst. **16**(4), 527–565 (2022)
10. Wang, Z., Zhu, H., Sun, L.: Social engineering in cybersecurity: effect mechanisms, Human vulnerabilities and attack methods. IEEE Access **9**, 11895–11910 (2021)
11. Bangda, B.: La cybercriminalité fait perdre 12,2 milliards au Cameroun en 2021. Eco-Matin. https://ecomatin.net/la-cybercriminalite-fait-perdre-122-milliards-s-au-cameroun-en-2021/. Accessed 01 Aug 2022
12. Gandotra, E., Gupta, D.: An efficient approach for phishing detection using machine learning. In: Giri, K.J., Parah, S.A., Bashir, R., Muhammad, K. (eds) Multimedia Security. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-8711-5_12
13. Do, N.Q., Selamat, A., Krejcar, O., Herrera-Viedma, E. and Fujita, H.: Deep learning for phishing detection: taxonomy, current challenges and future directions. IEEE Access 36429–36463 (2022)
14. Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., Shukla, S.: Applications of deep learning for phishing detection: a systematic literature review. Knowl. Inf. Syst. **64**, 1457–1500 (2022)
15. Quang, D.N., Selamat, A., Krejcar, O.: Recent research on phishing detection through machine learning algorithm. In: Fujita, H., Selamat, A., Lin, J.-W., Ali, M. (eds.) IEA/AIE 2021. LNCS (LNAI), vol. 12798, pp. 495–508. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-79457-6_42
16. Yu, T., Chen, X., Xu, Z., Xu, J.: MP-GCN: a phishing nodes detection approach via graph convolution network for ethereum. Appl. Sci. **12**, 7294 (2022)
17. Chen, W., Guo, X., Chen, Z., Zheng, Z., Lu, Y.: Phishing scam detection on ethereum: towards financial security for blockchain ecosystem. In: Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence Special Track on AI in FinTech, pp. 4506–4512 (2020)
18. Panga, R.C.T., Marwa, J., Ndibwile, J.D.: A game or notes? The use of a customized mobile game to improve teenagers' phishing knowledge. Case Tanzania. J. Cybersecur. Priv. **2**, 466–489 (2022)
19. Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., Furnell, S.: Evaluation of contextual and game-based training for phishing detection. Future Internet **14**, 104 (2022)
20. Ondrus, J., Pigneur Y.: An Assessment of NFC for future mobile payment systems. In: Proceeding of the International Conference on the Management of Mobile Business (2007)
21. Mbiti, I.M., Weil, D.N.: Mobile banking: the impact of M-Pesa in Kenya. NBER Working Paper No. w17129 (2011)
22. Téllez, J., Zeadally, S.: Mobile payment systems secure network architectures and protocols. Computer Communications and Networks, Springer (2017)
23. Bahri-Domon, Y.: Mobile money ready for take-off in cameroon, Mediamania. https://www.businessincameroon.com/pdf/BC28.pdf. Accessed 01 Aug 2022.
24. Mbodiam, B.R.: In Cameroon, MTN and orange wage a fierce commercial war on the mobile money market. https://www.businessincameroon.com/telecom/0202-6860-in-came-roon-

mtn-and-orange-wage-a-fierce-commercial-war-on-the-mobile-money-market. Accessed 01 Aug 2022
25. BRM: Cameroon: a decree to limit numbers of SIM per subscriber and prohibit sale of SIM cards on streets. https://www.businessincameroon.com/telecom/0110-5670-cameroon-a-de-cree-to-limit-numbers-of-sim-per-subscriber-and-prohibit-sale-of-sim-cards-on-streets. Accessed 01 Aug 2022
26. Orange, Transfert d'argent. https://www.orange.cm/fr/om-gestion-de-compte/transfert-d-argent.html. Accessed 01 Aug 2022
27. BRM: Mobile telephone subscribers' identification: telecom regulator ART admonishes cameroonian operators. https://www.businessincameroon.com/public-management/1204-11454-mobile-telephone-subscribers-identification-telecom-regulator-art-admonishes-cameroonian-operators. Accessed 01 Aug 2022
28. Atabong, A.B., Cameroon: SIM card shutdown piles on pressure for telcos. https://itweb.africa/content/lLn14Mmj9RKqJ6Aa. Accessed 01 Aug 2022
29. Johnson-laird, P.N., Oatley, K.: Basic emotions, rationality, and folk theory. Cogn. Emot. **6**(3–4), 201–223 (1992)
30. Bosamia, M.P.: MobileWallet payments recent potential threats and vulnerabilities with its possible security measures. In: Proceedings of the 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017), Changa, India, 1–2 pp. 1–7 (2017)
31. Mtaho, A.B: Improving mobile money security with two-factor authentication. Int. J. Comput. Appl. **109**, 9–15 (2015)
32. Bosamia, M.P.: MobileWallet payments recent potential threats and vulnerabilities with its possible security measures. In Proceedings of the 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017), Changa, India, vol. 1–2; pp. 1–7 (2017)
33. Saxena, S., Vyas, S., Kumar, B.S., Gupta, S.: Survey on online electronic payments security. In: Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, pp. 746–751 (2019)
34. Maseno, E.M., Ogao, P., Matende, S.: Vishing attacks on mobile platform in Nairobi county kEnya. Int. J. Adv. Res. Comput. Sci. Technol. **5**, 73–77 (2017)
35. Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., Dwomoh-Okudzeto, Y. Control of fraud on mobile money services in Ghana: an exploratory study. J. Money Laund. Control **22**, 300–317 (2018)
36. Gilman, L., Joyce, M.: Managing the risk of fraud in mobile money (2012). http://www.gsma.com/mmu. Accessed 01 Aug 2022
37. Lonie, S., Fraud risk management for mobile money: an overview (2017). https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf. Accessed 01 Aug 2022
38. Buku, M., Mazer, R.: Fraud in mobile financial services: protecting consumers, providers, and the system. https://www.cgap.org/publications/fraud-mobile-%EF%AC%81nancial-services. Accessed 01 Aug 2022
39. ITU, Security testing for USSD and STK based digital financial services applications. https://figi.itu.int/wp-content/uploads/2021/04/Security-testing-for-USSD-and-STK-based-Digital-Financial-Services-applications-1.pdf. Accessed 01 Aug 2022