Mobile Money & Social Engineering in Cameroon: Understanding Cyber Threats and Protection Strategies

- **Presented by:** Dr. Carlson Eyongabi
- **Date:** March 13, 2025
- FHNW University, Switzerland

University of Applied Sciences and Arts
Northwestern Switzerland

Topics:

- Understanding Mobile Money as used in Cameroon (Africa)
- Concrete Implementation of Mobile Money
- How Social Engineering Scams Exploit Mobile Money Users
- Case Studies: Real-Life Scams in Cameroon

University of Applied Sciences and Arts
Northwestern Switzerland

Mobile Money: Is a digital financial service that allows users to send, receive, and store money using their mobile phones. It is widely used across Africa for personal and business transactions.

MTN Mobile Money

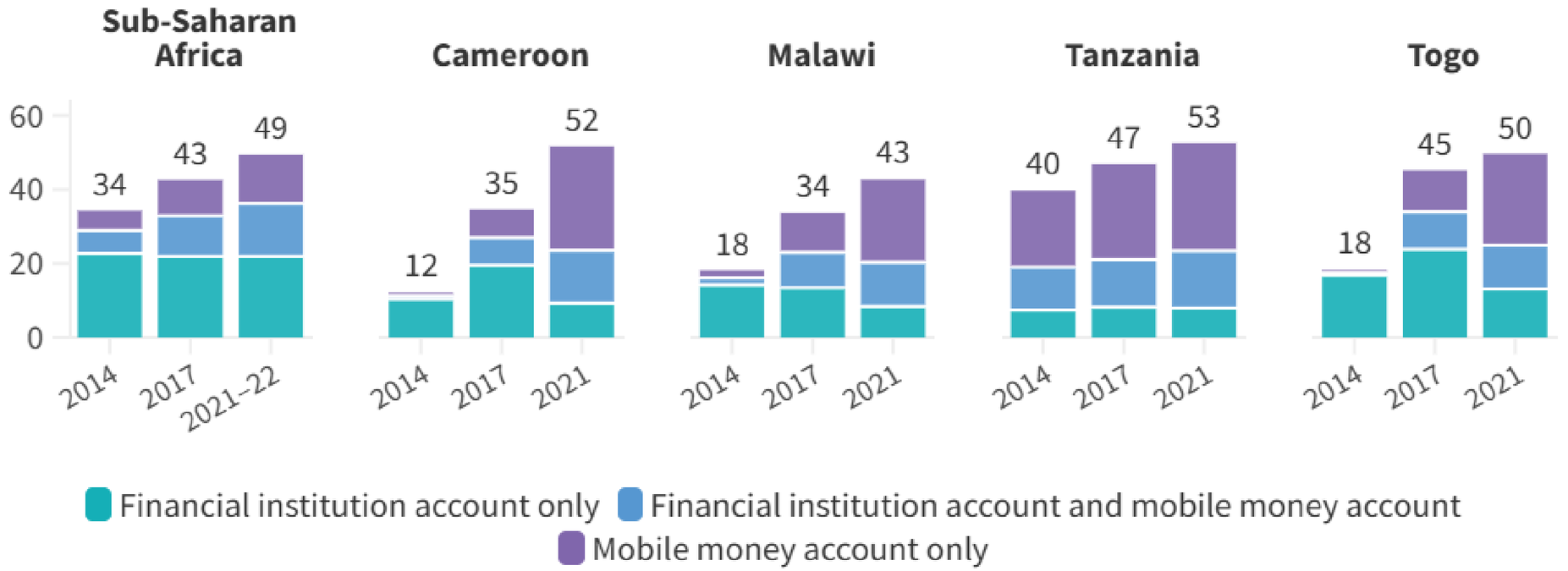
Orange Money

EU MOBILE MONEY

1. Introduction to Mobile Money

- Definition: Mobile Money refers to financial transactions conducted via mobile phones, including payments, transfers, savings, and loans.
- Importance: In Africa, Mobile Money has revolutionized financial inclusion, enabling millions without traditional bank accounts to access financial services.
- **Cameroonian Context**: Leading services include MTN MoMo, Orange Money, and Express Union Mobile. The **Ministry of Secondary Education in Cameroon adopted MTN Mobile Money for school fee payments**, reducing the need for physical queues and enhancing transparency

Mobile money usage in Cameroon has grown significantly, surpassing traditional banking services in terms of transaction volume. According to the **5th Cameroon Household Survey (Ecam 5)**, mobile money adoption among individuals aged 15 and older rose from **29.9% in 2017 to 42.7% in 2022**, marking a **12.8% increase** over five years. The COVID-19 pandemic played a significant role in accelerating this shift, as government measures encouraged digital financial transactions to reduce cash handling.



Source: Global Findex 2021

WORLD BANK GROUP

Key players in the mobile money market include **MTN Cameroon** and **Orange Cameroon**, with Camtel planning to launch its own service, **"Blue Money."** These services are widely used for peer-to-peer transfers, bill payments, and even tax payments.

In the **CEMAC region:**

- Mobile money dominates financial transactions, accounting for **96% of all transactions (2.3 billion operations)**
- **T**raditional banking methods like card payments and bank transfers only make up **2% (48.3 million operations)**. However, in terms of transaction value, traditional banking still leads, handling **44% of total transaction value** (CFA 48,573 billion), while electronic currency transactions account for **21%** (CFA 23,332 billion).

Cameroon is the top country in the region for both transactions, executing **71% of total transactions (1.7 billion)** and **55% of transaction value (CFA 59,003 billion)**

Source: https://www.businessincameroon.com/

Mobile Money usage surges in Cameroon, outpacing traditional banking

MTN Mobile Money

Orange Money

EU MOBILE MONEY

What is Twint? (Switzerland)

Swiss mobile payment app linked to bank accounts and credit cards.
Used for:

- ❖ Peer-to-peer transfers
- ❖ Online & in-store purchases
- ❖ Parking, e-commerce, and vending machine

Comparison: Mobile Money vs. Twint

Feature	Mobile Money (Cameroon)	Twint (Switzerland)
Main Users	Unbanked & banked users	Mostly banked users
Registration	Phone number-based	Bank account-linked
Transaction Method	USSD & app-based	App-based
Security Risks	SIM swap, social engineering fraud	Phishing, account takeover
Common Scams	Fake deposits, reversal scams	Fake invoice & refund scams

📌 *How do you think digital payments differ in Switzerland vs. developing countries like Cameroon?*

Concrete Implementation) MTN Mobile Money (aka MoMo)

Concrete Implementation) MTN Mobile Money (aka MoMo)

1. Registration

To use MTN MoMo, you need to:

- Have an MTN SIM card.
- Register at an MTN MoMo agent or via USSD/SMS.
- Provide a valid ID for verification.

2. Depositing Money (Cash-In)

- Visit an MTN MoMo agent.
- Give cash to the agent.
- The agent transfers the equivalent amount to your MoMo wallet.

3. Sending & Receiving Money

- Dial *# (country-specific MoMo USSD code)* or use the MoMo app.
- Choose "Send Money" and enter the recipient's phone number.
- Confirm the transaction with your MoMo PIN.
- The recipient gets an instant notification.

4. Withdrawing Money (Cash-Out)

- Visit an agent or ATM (where available).
- Select "Withdraw Money" on the MoMo menu.
- Enter the agent's phone number and the amount.
- Confirm with your PIN.
- The agent gives you the cash.

5. Paying Bills & Services

MTN MoMo can be used to:

- Pay utility bills (electricity, water, internet, etc.).
- Buy airtime and data.
- Pay for goods and services at MoMo merchants.

6. Saving & Loans (Available in Some Countries)

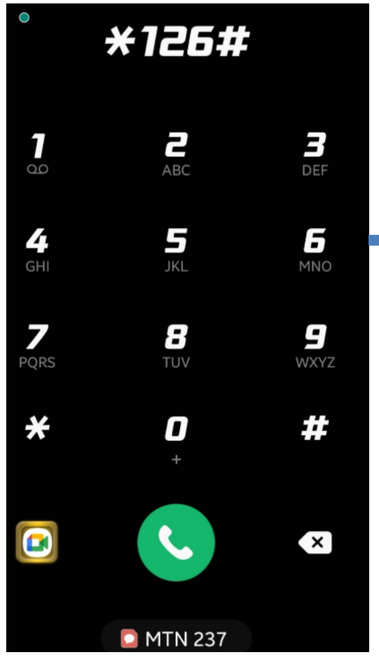
- Users can save money in their MoMo wallet.
- Some countries offer MoMo loans and microcredit services.

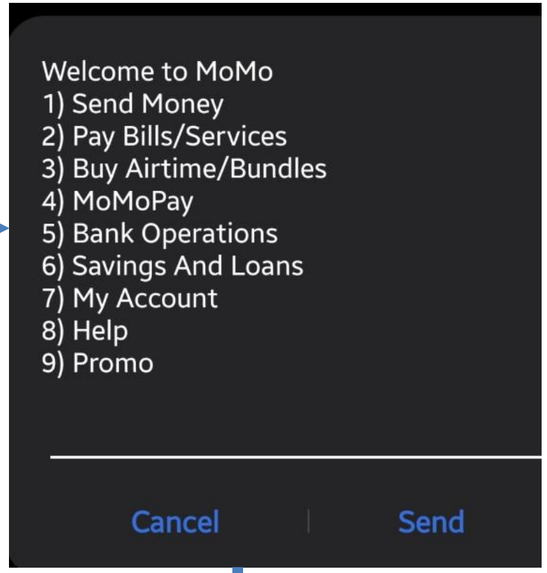
7. Security Features

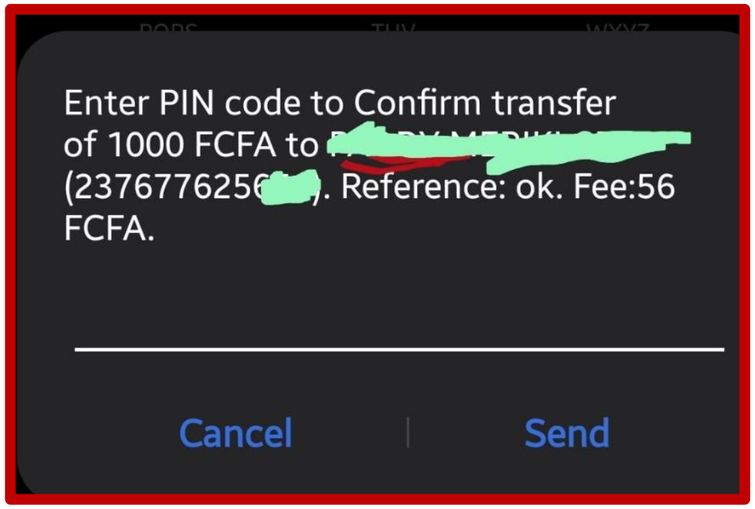
- Transactions require a secret PIN.
- SMS notifications confirm every transaction.
- Fraud prevention measures include MoMo agent verification.

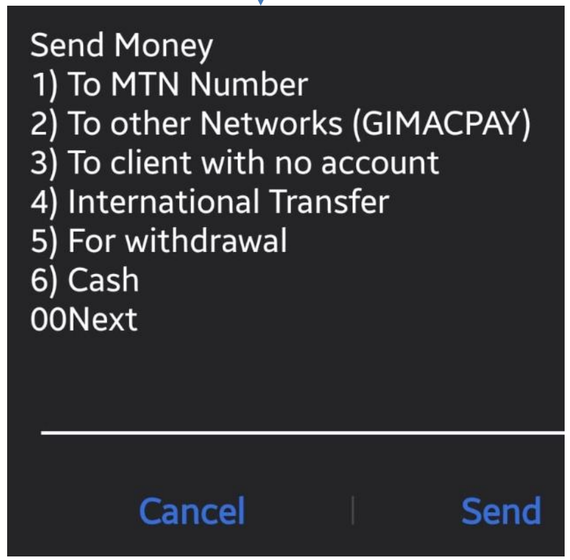
Mobile Money Works in Cameroon (MTN MoMo)

- **USSD Technology:**
  - USSD (Unstructured Supplementary Service Data) is the backbone of Mobile Money in Cameroon.
  - Users dial short codes (e.g., *126#) to access services.
- **GSM Network:**
  - USSD operates over the GSM signaling channel, enabling real-time communication without the internet.
- **Transaction Flow**
  - User → USSD code → GSM network → Mobile Money server → Response.



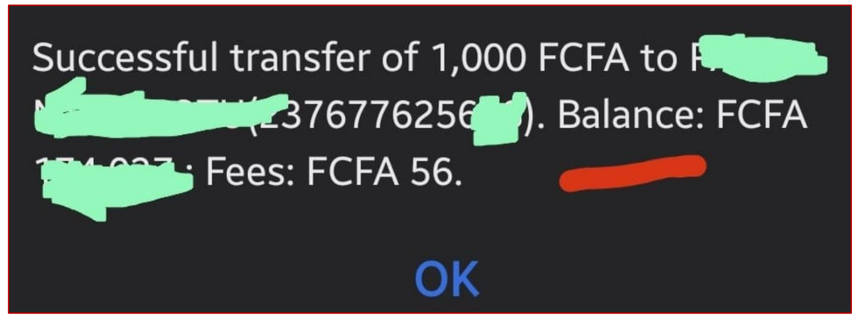




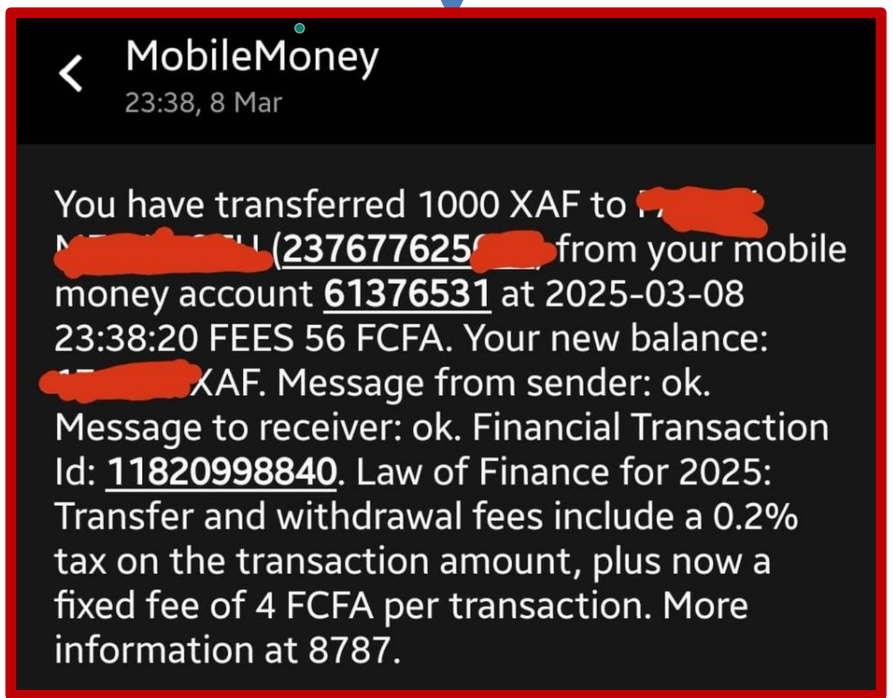


Mobile Money USSD Transactions vs. SMS Transaction Messages

- **USSD Transactions:**
  - Real-time, interactive sessions initiated by the user.
  - Used for sending money, checking balances, and paying bills.
  - Vulnerable to **SIM swap attacks** and **USSD code spoofing**.
  - Using SS7 exploits, a fake base station, or malware, the hacker intercepts the USSD session.
- **SMS Transaction Messages:**
  - One-way notifications sent by the Mobile Money operator.
  - Used to confirm transactions, share OTPs, and provide account updates.



SMS Response



- **Comparison Table:**

Feature	USSD Transactions	SMS Transaction Messages
Purpose	Interactive transactions	Transaction notifications
Initiated By	User	Mobile Money operator
Security Risks	SIM swap, USSD spoofing	SMS interception, smishing
Encryption	Typically unencrypted	Often unencrypted

How Social Engineering Scams Exploit Mobile Money Users

Authentication & Authorization

- **Personal Identification Number (PIN)**: Every transaction requires a secret PIN to prevent unauthorized access.
- **Two-Factor Authentication (2FA)**: ~~Some MoMo services implement additional authentication for higher security.~~

Secure USSD Communication

- **USSD messages are not stored on the device**: This reduces the risk of message interception on the phone.
- **Session-based security**: USSD transactions occur in real-time, and the session ends after a short period, minimizing risks.

- **USSD (Unstructured Supplementary Service Data)** – Used for transactions via feature phones without internet access.
- **SIM Toolkit (STK)** – Pre-installed on SIM cards, enabling MoMo services through menus.

MTN MoMo transaction notifications are often sent via **plain text SMS**, which inherently lacks encryption. While MoMo itself uses **secure encryption protocols** during transactions, the final SMS notification to the user is a potential security weak point

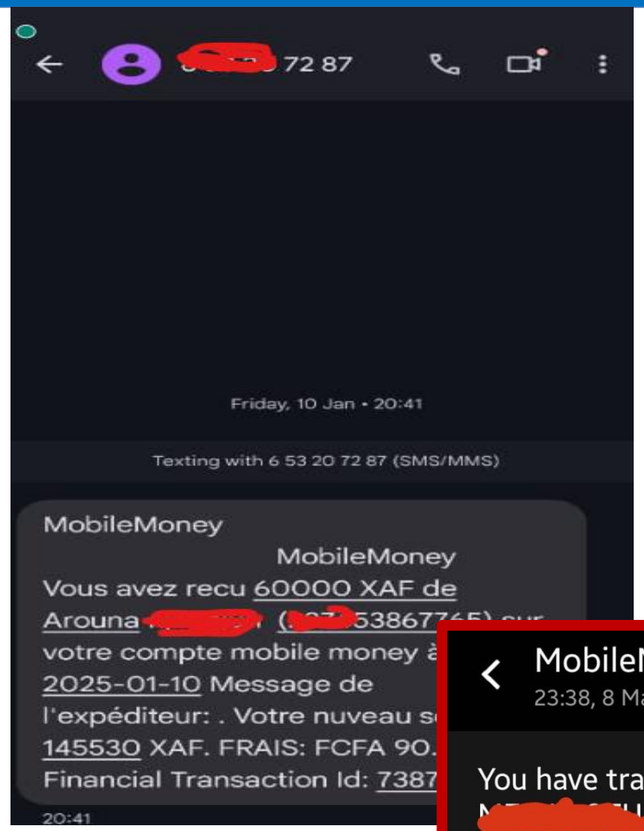
1. SMS is Not Encrypted, But Risk is Mitigated

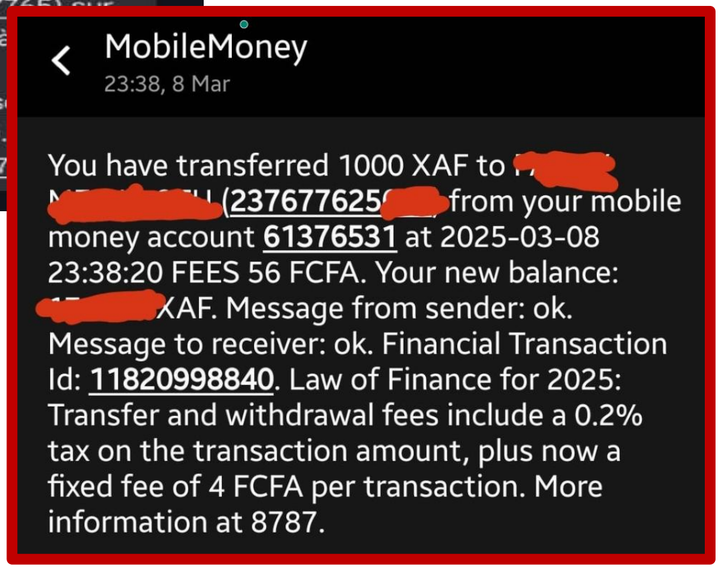
- **Why SMS is used:** Many users, especially in areas with limited internet access, rely on basic feature phones, making SMS the most accessible notification method.
- **Risk:** SMS messages can be intercepted by attackers using SIM swap fraud, SS7 protocol vulnerabilities, or phone malware.

2. Other Security Layers That Reduce Risk

Even though SMS notifications are in plain text, MTN MoMo employs:

- **PIN-based Authentication:** The most critical security layer is the requirement to enter a secret PIN before a transaction is processed. Even if someone sees an SMS, they cannot initiate unauthorized transactions without the PIN.
- **Real-time Fraud Monitoring:** Suspicious transactions trigger alerts and may require additional verification.
- **Time-sensitive Session Security (for USSD & App):** Transactions occur in temporary sessions that expire after a short period, reducing exposure to attacks.





Social Engineering and Cybersecurity Threats in Mobile Money

Social engineering exploits human psychology to manipulate users into divulging confidential information. In the context of Mobile Money, common threats include:

A. Phishing Attacks

- Fake SMS or emails pretending to be from Mobile Money providers (e.g., MTN or Orange) requesting login credentials.
- **Example:** A fraudster sends a message claiming the user has won a lottery and must enter their PIN to claim the prize.

B. SIM Swapping

- Attackers convince telecom providers to issue a duplicate SIM card, gaining access to a victim's Mobile Money account.

C. Fake Customer Support Scams

- Fraudsters pose as Mobile Money customer service agents, requesting users to share their OTP (One-Time Password) or reset PINs
- **Tactic:** Scammers call users pretending to "fix an issue" with their account but actually hijack it.

D. Insider Threats

- Employees at telecom or financial institutions leaking customer data to fraudsters.
- **Example:** In some cases, bank employees have been bribed to reset PINs or approve unauthorized transactions.

Tools and Techniques to intercept SMS messages

1. SIM Swap Fraud (SIM Jacking)

How It Works

- **Social Engineering or Insider Threats**: Hackers gather personal details (**name, phone number, ID**) from social media, phishing attacks, or corrupt telecom employees.
- **Fake SIM Replacement Request**: They contact the mobile service provider, **claiming a lost SIM** and request a new one.
- **Taking Over the Phone Number**: Once the hacker gets a **replacement** SIM, they start receiving SMS messages, including MoMo transaction notifications and OTPs (One-Time Passwords).
- **Account Hijacking**: With access to SMS, they reset passwords on banking, MoMo, and email accounts.

Tools Used

- **Caller ID Spoofing Apps (e.g., SpoofCard, Hushed)** – Trick customer service into thinking the request is from the real owner.
- **Data Brokers & Dark Web Databases** – Hackers buy leaked personal details to convince telecom companies.

How to Prevent It

- ✔ **Enable SIM Lock (PIN-protected SIM card).**
- ✔ **Use Multi-Factor Authentication (MFA) that doesn't rely on SMS (e.g., Authenticator Apps).**
- ✔ **Set up a security question or PIN with your mobile provider.**

Tools and Techniques to intercept SMS messages

2. SS7 Attack (Signaling System No. 7 Exploit)

How It Works

SS7 is a global telecom protocol that allows networks to communicate. Hackers exploit SS7 vulnerabilities to:

- **Intercept SMS Messages**: Once access is gained to SS7, attackers can reroute text messages (MoMo alerts, OTPs) to their devices.
- **Eavesdrop on Calls**: They can listen to conversations or redirect them.
- **Fake Transactions**: With access to OTPs, they can reset passwords or authorize MoMo transfers.

Tools Used

- **Sigploit** – A penetration testing tool for SS7 vulnerabilities.
- **SnoopSnitch** – An Android app that detects SS7 attacks.
- **Hacked SS7 Access (Available on the Dark Web)** – Cybercriminals buy access to global telecom networks.

How to Prevent It

- ✔ **Use MoMo app push notifications instead of SMS OTPs.**
- ✔ **Use an encrypted messaging service like Signal for important financial communications.**
- ✔ **Telecom providers should upgrade to Diameter Protocol (an SS7 replacement with better security).**

Tools and Techniques to intercept SMS messages

3. Malware-Based Attacks (Spyware & SMS Forwarding Trojans)

How It Works

- ❖ **Infecting the Victim's Phone**: Hackers trick users into installing a malicious app (disguised as a MoMo loan app or free VPN).
- ❖ **Stealing SMS Messages**: The malware silently forwards all SMS messages (including MoMo notifications) to the hacker's number.
- ❖ **Hijacking MoMo Transactions**: Some advanced malware can even initiate transactions without user knowledge.

Tools Used

- ❖ **FlexiSPY & mSpy** – Commercial spyware used for SMS monitoring.
- ❖ **Android RATs (Remote Access Trojans) like SpyNote & AndroRAT** – Allow hackers to control infected phones remotely.
- ❖ **Malicious Apps on Third-Party Stores** – Fake MoMo or financial apps designed to steal credentials.

How to Prevent It

- ✔ **Only install apps from official stores (Google Play Store, Apple App Store).**
- ✔ **Check app permissions – Avoid apps that request access to SMS without a valid reason.**
- ✔ **Keep your phone updated with the latest security patches.**

Tools and Techniques to intercept SMS messages

5. Man-in-the-Middle (MitM) Attacks on Public Wi-Fi

How It Works

- **Hacker Creates a Fake Wi-Fi Hotspot**: Victims unknowingly connect to a free Wi-Fi network in places like airports or cafés.
- **Intercepting SMS & Online Transactions**: The hacker uses tools to capture unencrypted traffic, including SMS messages sent over VoIP services.
- **Stealing Login Credentials & MoMo OTPs**: If the user logs into their MoMo account, the attacker can capture credentials.

Tools Used

- **Wireshark** – Used to analyze network traffic.
- **Ettercap** – Performs ARP spoofing to intercept unencrypted data.
- **Evil Twin Attack Kits (e.g., Wifiphisher)** – Creates fake Wi-Fi hotspots.

How to Prevent It

- ✔ **Avoid logging into MoMo or financial accounts over public Wi-Fi.**
- ✔ **Use a VPN to encrypt internet traffic.**
- ✔ **Use cellular data (3G/4G) instead of public Wi-Fi for sensitive transactions.**

Overpayment or Reversal Scam Works in Mobile Money Fraud

1. Fraudster Sends Fake Money to Your Account

- The scammer **sends a fake or invalid transaction notification** to your phone.
- They often use **spoofing techniques** to make it look like a legitimate mobile money transfer.
- Some fraudsters actually deposit money but use a stolen or fraudulent source.

2. Fraudster Contacts the Victim (You)

- Immediately after sending the fake transaction, the scammer **calls or messages you**, pretending to be a distressed individual.
- They claim that they **sent money to your account by mistake** and urgently need it back.
- Some even impersonate **mobile money customer service** and claim they are helping another customer retrieve lost funds.

3. The Pressure Tactic

- The scammer **pressures you to act quickly**, often saying:
  - “It was meant for my sick mother.”
  - “It was my boss’s money, and I’ll get fired.”
  - “Please return it before my account is blocked!”
- The fraudster tries to create a **sense of urgency**, preventing you from checking whether the transaction was genuine.

Understanding Mobile Money in Cameroon vs. Switzerland

- **How do you normally make small everyday payments in Switzerland?** (e.g., cash, Twint, credit cards?)
- **What are the key differences between Mobile Money in Cameroon and digital payment systems like Twint in Switzerland?**
- **Do you think a system like MTN MoMo could be successful in Switzerland? Why or why not?**

Precautions to Minimize Cyber Risks

Potential Security Risks

- ❖ Never share their PIN with anyone.
- ❖ Avoid responding to phishing messages or fraud calls.
- ❖ Only use official MTN MoMo agents and platforms.
- ❖ Be cautious of phishing scams and SIM swap fraud.
- ❖ Confirm amount, number and name of recipient before approving a transaction

Case Studies: Real-Life Scams in Cameroon

Case Study 1: MoMo Agent Fraud – Douala (2023)

- In **2023**, a fraud ring in **Douala** exploited MoMo agents by pretending to be legitimate customers.
- They would **generate fake transaction SMS messages** and convince agents to hand over cash.
- Losses were estimated at **50 million FCFA** before authorities intervened.

Case Study 2: SIM Swap Fraud – Yaoundé (2022)

- In **2022**, a businessman in **Yaoundé** lost **2 million FCFA** after scammers cloned his SIM card.
- The criminals **reset his MoMo PIN** and withdrew funds from his account.
- **How did it happen?**
  - The scammer **used fake ID documents** to convince a telecom agent to issue a new SIM card.
  - Once activated, they accessed the victim's MoMo account and emptied it.

Case Study 3: Fake MoMo Deposit Scam – Bamenda (2021)

- A woman in **Bamenda** lost **500,000 FCFA** after receiving a **fake deposit SMS**.
- The scammer, posing as a relative, asked her to refund the "mistaken deposit."
- Since she trusted the sender, she **sent the money before verifying**.

Regulations on Mobile Money

- The Bank of Central African States (**BEAC**) regulates mobile money operations within the CEMAC region (which includes Cameroon). The **Regulation No. 2/18/CEMAC/UMAC/CM** sets rules on electronic payments and financial transactions, ensuring that mobile money services adhere **to anti-money laundering (AML)** and financial integrity measures
- The **Central African Banking Commission (COBAC)** also supervises mobile money providers to ensure compliance with financial regulations and prevent fraud.

•Cybersecurity and Mobile Money in Cameroon

- The **National Agency for Information and Communication Technologies (ANTIC)** is responsible for cybersecurity in Cameroon. It has been working to curb **cyber threats, including those targeting mobile money users**.
- According to the **National Agency for Financial Investigation (ANIF)**, cybercriminality related to mobile money transactions has been increasing in Cameroon, especially after previous cases of fund misappropriation

•Challenges and Risks

- Despite regulations, mobile money users remain vulnerable to fraud, SIM swap attacks, and social engineering scams. Cybercriminals exploit weak security measures, often tricking users into revealing PIN codes or intercepting SMS-based transaction confirmations.

• Government and ANTIC's Response

- ANTIC has been involved in public awareness campaigns to educate mobile money users on cybersecurity best practices.
- The Cameroonian government has also been working on strengthening digital financial regulations to mitigate fraud risks.

📜 References & Sources

1. GSMA Mobile Money Report 2023 – www.gsma.com
2. MTN Cameroon Fraud Warnings – www.mtn.cm
3. ANTIC Cybersecurity Reports 2023 – www.antic.cm
4. Orange Money Cameroon Security Guide – www.orange.cm
5. Mobile Money Africa https://mobilemoneyafrica.com/blog/cameroon-mobile-money-outpaces-traditional-banking
6. Doing Business in Cameroon https://www.businessincameroon.com/finance/2604-13791-mobile-money-usage-surges-in-cameroon-outpacing-traditional-banking

Thank You!

Questions ???

CARLSON EYONGABI NGWA

SENIOR PROJECT MANAGER / DIGITAL BUSINESS PARTNER AT ATOS AG ON CLIENT PROJECTS

Nationality: CMR/CH

Address: Bühlerweg 12B, 5702 Niederlenz
Switzerland
Phone: +41 76 54 88001
Email: carlson@ngwa.ch

EDUCATION

Doctor of Management in Information Systems and Technology
University of Phoenix, Phoenix, AZ, USA
2009 – 2012

MSc in Information Technology
University of Derby, Derby, UK
2003 - 2005