Vishing-Based Mobile Money Fraud in Ghana
An Investigation into Voice Phishing, Insider Threats, and Systemic Weaknesses in Mobile Money

Executive Summary

This case study explores the rise of vishing-based fraud in Ghana, particularly targeting MTN Mobile Money (MoMo) users. It investigates how threat actors exploit Social engineering, insider leaks, and weak fraud reversal protocols to steal from unsuspecting victims. Through scenario modeling, legal analysis, and practical recommendations, this report outlines a robust, multi-layered defense strategy. The aim is to strengthen digital financial security while raising awareness among users, telecoms, and regulators. This case study is presented as a cybersecurity portfolio project to demonstrate technical insight, social awareness, and problem-solving ability.

Skills Demonstrated

- Threat Analysis
- Risk Assessment
- Security Strategy
- Policy Awareness
- Communication
- Documentation

Real-World Scenario: Victim Persona

Victim: Ama, a 48-year-old trader in Accra
Incident: She receives a call on her birthday. The caller, claiming to be from MTN, tells her she's won a birthday promotion. They know her name and her last MoMo transaction (leaked by a rogue vendor). To receive the prize, she's asked to "confirm her PIN." Moments later, all her funds are transferred to a Vodafone wallet and unrecoverable.
Impact: Financial loss. Emotional distress. No recovery support.

Key Findings

- Threat Actors use vishing (voice phishing) tactics to manipulate victims using personal data and social engineering.
- Insider Threats from MoMo vendors and even MTN staff leak transaction data to fraudsters.
- Regulatory gaps and weak reversal systems allow cross-network fraud to succeed.
- Low user awareness and limited incident reporting mechanisms worsen the problem.

Common Vishing Scenarios (Social Engineering)

1. **Fake Promotions or Rewards**
    - Scammers impersonate MTN and claim you've won a promotion or birthday gift. They ask for your MoMo PIN or prompt you to approve a withdrawal.
2. **Mistaken Transfers**
    - A fraudster pretends to have mistakenly sent money to your wallet and asks you to return it. In reality, no such transaction occurred, and the victim ends up transferring their own funds.
3. **POS-based PIN Theft**
    - Dishonest MoMo vendors watch or record your PIN during withdrawals, then later clone your SIM or leak details to accomplices.
4. **SIM Swap and Identity Theft**
    - Scammers collect personal details through fake calls, then collaborate with insiders to execute unauthorized SIM swaps and drain mobile wallets.
5. **Scam**
    - Fraudsters call to deceive subscribers that they are to deliver goods from Abroad or from a close relative under false pretext. Some fraudsters call and ask for money to be deposited in mobile money account in exchange for goods from relatives or friends from abroad. ie Popular “sister nie oo”

Insider Threats in Vishing-Based Mobile Money Fraud

While most vishing attacks appear to originate externally, insider threats within the mobile money ecosystem play a major enabling role. Some MTN staff and Mobile Money (MoMo) vendors have been implicated in the unauthorized sharing or sale of customer data to fraudsters.

How Insider Threats Enable Vishing Scams

- **Transaction history** is leaked, allowing scammers to sound credible when referencing recent activities.
- **Contact information** is shared, letting scammers directly target users with personalized calls.
- **SIM registration or KYC data** is exposed, aiding in identity theft or SIM swaps.
- **Bypassing internal security** with the help of rogue insiders facilitates unauthorized account resets.

Insider Threat Chain

[Vendor/Staff Leak] → [Threat Actor Call] → [Victim Deceived] → [Fraud Successful]

Impact

These actions significantly increase the success rate of vishing scams because victims are more likely to trust calls that appear authentic and data-driven.

Recommendations

1. **Enhanced Vendor and Staff Vetting**
    - Thorough background checks and ongoing monitoring.
2. **Behavioral Logging and Monitoring**
    - Audit access to customer data and flag anomalies.
3. **Strict Legal Sanctions**
    - Immediate termination, blacklisting, and prosecution under Ghana's Data Protection Act.
4. **Anonymous Reporting Channels**
    - Encourage employees and vendors to report suspected insider involvement confidentially.
5. **Mandatory Cybersecurity Training**
    - Regular training on fraud prevention and privacy laws for all vendors and staff.

Proposed Countermeasures

To effectively combat vishing-based mobile money fraud, a multifaceted response is required:

1. **User Education Campaigns**
    - Partner with churches, mosques, schools, and media to raise awareness, especially among the digitally vulnerable.
    - Local language radio dramas and jingles that share real-life stories and tips in an entertaining format.
2. **Telco Collaboration**
    - MTN and other providers must share fraud intelligence and implement unified fraud detection and reporting protocols.
3. **Improved Fraud reports and resolution Systems**
    - Enable real-time cross-network reversal capabilities to reduce stolen fund extraction.
    - MTN and other providers must share fraud intelligence and implement unified fraud detection and reporting protocols
    - Set up 24/7 dedicated call center number extension to handle real time reports of Momo fraud incidents with real urgency to help resolve cases on time and ensure public trust in the system
4. **Stronger Verification for SIM Swaps**

- Implement stricter checks before allowing any SIM change.

5. **Incentivize Whistleblowers**
   - Offer financial rewards and anonymity for insiders who report fraud.
6. **Regulatory Compliance and Oversight**
   Enforce strict adherence to Ghana's Data Protection Act, Electronic Transactions Act, and Bank of Ghana's cybersecurity directives.
   - Telecoms must log and report fraud attempts.
   - Mobile money agents should be regularly audited and certified.
   - Regulatory bodies must issue penalties for non-compliance and establish an independent oversight body for mobile money fraud.

Cybersecurity Maturity Heatmap (Summary)

Domain	Status	Comments
User Awareness	🔴 Low	Many victims unaware of voice scams
Insider Threat Protection	🟠 Medium	No vetting or monitoring systems
Fraud Reversal Protocols	🔴 Very Weak	Reversal almost impossible cross-net
SIM Swap Verification	🟡 In Progress	Biometrics not fully enforced
Regulatory Enforcement	🟠 Medium	Laws exist but enforcement is limited

Appendix: Regulatory Framework Summary

Law/Directive	Focus	Relevance
Data Protection Act, 2012 (Act 843)	Privacy, data control	Penalizes vendor/staff data leaks
Electronic Transactions Act, 2008 (Act 772)	Unauthorized access, fraud	Covers SIM swap, fake reversal scams
BoG Cybersecurity Directive (2023)	Incident reporting, audits	Requires fraud logs and 24h reporting
Payment Systems and Services Act, 2019 (Act 987)	Electronic payments, fraud prevention, consumer protection, AML compliance	Requires fraud detection, consumer protection, and AML compliance from mobile money providers. Ensures secure payment systems through licensing and oversight.
NCA SIM Registration Regulations	Biometric identity verification	Prevents fraudulent SIM swaps

Contact Information

Name: Bernard Arthur

Email: Bernnardarthur@gmail.com