



THE QUEST FOR CYBER SECURITY TO COMBAT THREATS TO DIGITAL FINANCE IN UGANDA



Unleashing Potential

AUTHORS:

Joseph Kayemba
Jonah Kiberu



This work is licensed under a Creative Commons Attribution -NonCommercial 4.0 International License

MAY 2023

<https://gatewayresearchcentre.org/>

Executive Summary

The Police have recorded an increase in the cybercrimes cases from 256 to 286 between 2020 and 2022 which is 11.7% increment.

Banks and telecom companies have become a target for cybercriminals such as hackers, phishers and fraudsters as Ugandans have increased to use these avenues to transact, make e-payments and e-savings as they are convenient and time saving. Cybercrimes have greatly increased most especially from 2020 to date due to the fact that Covid-19 broke out in 2020 a period in which there was restricted movement and following of advice from the Ministry of Health to avoid physical exchange of money as this was also a channel through which the pandemic would rapidly spread. Since most of the business people and the corporates had mobile phones, they highly adopted electronic means such as mobile money, online banking and mobile banking to avoid being infected with the disease hence increased usage of the digital financial services. For the cybercriminals were also on the look out to use this opportunity to steal peoples' money. Since then, the Police have recorded an increase in the cybercrimes cases from 256 to 286 between 2020 and 2022 which is 11.7% increment. For instance, ***Uganda Police Force Annual Crime Report 2022 indicated that cybercrimes led to a loss of***

Ugx.19,209,798,000 in 2022, out of which Ugx.16,790,000 was recovered implying that 99.91% of the money lost was not recovered. To the victims, this is a huge loss hence mistrust in the digital financial institutions since the recovery rate of the lost money is next to none. These emerging threats such as digital fraud, compromise of mobile money accounts and banking apps have made digital financial services risky and untrusted. Even though digital fraud has increased, digital literacy has remained low as the responsible parties such as Bank of Uganda, Financial Institutions (Banks and Microfinance) and telecom companies have not equally sensitized and educated the public on emerging digital threats and how to combat them.

It is recommended that Bank of Uganda should put more effort to manage Digital financial risks and ensure financial stability to empower Ugandans with a broad range of innovative e-payment options which are safe, efficient, accessible, and inclusive to promote social economic transformation and financial freedom, provide guidance on cyber defenses,

Scammers acquaint themselves with how a system works and its loopholes. Often times they conspire with employees or former employees of banks or telecom companies to syndicate their illegal financial deals.

conduct Annual IT Systems Audits (twice a year for banks and telecom companies), Consumer empowerment through digital finance literacy, deploy Policy Think Tanks that can conduct research in line with digital finance and as well promote stake holder collaboration between BOU, UCC, NIRA, Police and consumers).

Introduction

In this contemporary world, life and technology are inseparable. This is one of the elements of quantum computing under the fourth industrial revolution (Klaus S, 2016)¹. People work hard to earn but issues arise during transacting and saving their money. In Uganda, digital transactions and savings are executed using banks, mobile money transfers, and digital money apps or remittance platforms. However, hackers, fraudsters and conmen are on the look out to digitally defraud people. Since Mobile money and banks digitally manage finance, cyber criminals target accounts of individuals, companies, organizations, and government entities to steal money using computers and electronic gadgets.

Computer literates (techies / technophiles) use the vulnerabilities and loopholes in the financial management systems of banks and mobile money to accomplish illegal financial transactions by withdrawing or transacting money to the accounts of scammers. To accomplish this, scammers acquaint themselves with how a system works and its loopholes. Often times they conspire with employees or former employees of banks or telecom companies to syndicate their illegal financial deals. In this kind of scams, it is the clients that suffer most since intruders tamper with their accounts making it hard to recover colossal sums. ***The trauma that clients encounter has created mistrust in banks, telecom companies, and digital money apps to cease from being the safest avenues to keep money and carry out transactions.*** The major digital financial risks include hacking using spyware, phishing, identity theft, PIN theft, key-logging, hidden transaction costs, and failed transactions with no refund, which are worsened by delayed or no support from service providers (BOU, 2022)²

¹ Klaus S (2016) The Fourth Industrial Revolution: *World Economic Forum*. Available on: https://law.unimelb.edu.au/data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf

² Bank of Uganda (2022) Digital Financial Literacy (DFL) Module: *Strategy for Financial Literacy in Uganda*, Available on <https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/FinancialInclusion/Digital-Financial-Literacy-Core-Message-2023...pdf>

Again clients are shifting back to traditional means of keeping money in wallets or at home in wooden boxes, under the beds and physical movement with cash which exposes them to theft and robbery. These weaknesses undermine the basis for digital financial services in Uganda that necessitate policy interventions and technological reforms.

Cybercrimes in Uganda

The Uganda Police Force Annual Crime Report (2022) indicates 286 cases of Cybercrimes reported to the Police compared to 258 cases in 2021, implying a 10.8% (28 new cases) increase in this crime category. By the end of 2022, 45 cases were taken to Court, 09 cases were not proceeded with while 232 cases are still under inquiry. Out of the total cases taken to Court, 05 cases secured convictions, 01 case was dismissed while 39 cases are pending in Court which is a high case backlog. Cybercrimes led to a loss of Ugx. 19,209,798,000 in 2022, out of which Ugx. 16,790,000 was recovered. This implies 99.91% of the money lost was not recovered. To the victims, this is a huge loss hence mistrust in digital finance systems due to a low recovery rate of the lost money. Even though digital fraud has continued, Police, Bank of Uganda, commercial banks and telecom companies still have loopholes in their security measures to avert digital theft or

apply rigorous efforts to recover victims' lost money. Since the money lost is not fully recovered, this is an indicator that the forensic teams of police, telecom companies and Banks are wanting. ***The loopholes in the digital financial management systems have paved an opportunity to the hackers and fraudsters to engineer their actions.*** Approximately 74.45% of Ugandans live in rural areas (World Bank Development Indicators,2023). They would use their mobile phones to transact and save using mobile money and mobile banking, but most of them fear to use them due to limited safety. To Uganda's economy, this thwarts the revenue base and violates the financial freedom of the population.

A 2020 report by the Police's Criminal Investigations Directorate (CID) revealed that at least Shs5 billion was fraudulently sent to 877 Airtel Uganda Sim Cards while 755 MTN Sim Cards fraudulently received at least Shs5. 5 billion via mobile money by scammers.

Cybercrimes led to a loss of Ugx. 19,209,798,000 in 2022, out of which Ugx. 16,790,000 was recovered. This implies 99.91% of the money lost was not recovered. To the victims, this is a huge loss hence mistrust in digital finance systems due to a low recovery rate of the lost money.

In Table 1 below, there was an increase in mobile money subscribers and transactions between 2020 and 2022. Therefore, this calls for strengthening of digital security measures to secure transactions and protect clients from fraudsters who target less informed customers and loopholes in e-money systems.

Mobile Money Statistics (2020-2022)³

Year	2020	2021	2022	% increase from 2020-2022
No. of transactions	3,526,972,165	4,290,780,097	5,230,548,350	48.3%
Value of transactions (UGX)	93,728,611,507,775	138,920,750,686,578	165,614,789,577,132	76.6%
No. of registered customers	30,735,167	32,762,369	40,891,557	33%

Source: Bank of Uganda website

The above statistics show that mobile money usage and mobile money transfers have greatly increased in Uganda.

A total of 4,143 cases of mobile phone theft were reported in 2021 compared to 4,043 cases reported in 2020, showing a 2.4 percent increase. Most of the cases were a result of snatching from unsuspecting members of the public according to the 2021/2022 police report. The Uganda Police Annual Crime and Road Safety Report of 2019 showed more than 41 billion Ugandan Shillings (\$11m) was lost to criminals through cybercrimes including swapping SIM cards and hacking digital financial accounts last year⁴.

³ <https://www.bou.or.ug/bou/bouwebsite/PaymentSystems/dataandstat.html>

⁴ <https://www.upf.go.ug/wp-content/uploads/2023/02/OFFICIAL-ANNUAL-CRIME-REPORT-2022-Web-Version.pdf?x89335>

Why Cybercrimes have increased

Cybercrimes have greatly increased most especially from 2020 to date partly due to Covid-19 pandemic that broke out in 2020 a period characterized by restricted movements and massive lay off of employees by a multiplicity of organizations, rendering them unemployed. Similarly, the Ministry of Health advised citizens to (if possible) restrain from physical exchange of money as this was also a channel through which the pandemic would rapidly spread. Since most of the business people and corporates had mobile phones, they highly adopted electronic means such as mobile money, internet banking and mobile banking to avoid exposure to the disease. This partially increased the usage of digital financial services in addition to households receiving money from relatives and friends in distant places. After Covid-19 lockdowns, people were used to digital finance and have continued to use digital services. Digital financial usage increased but banks, police and telecom companies didn't equally bolster digital security and less effort invested to educate the public on how to combat and avoid digital financial fraud. With such weaknesses in the systems, cybercriminals are always on the look out to steal peoples' money.

Digital financial usage increased but banks, police and telecom companies didn't equally bolster digital security and less effort invested to educate the public on how to combat and avoid digital financial fraud.

The increased use of digital financial services such as Fintechs, Mobile money, Digital Credit, Digital payments, digital savings, investments, and remittances, Agent Banking and Card Payments have resulted in emerging threats like Digital Fraud, Social engineering, Compromise on banking Apps, Sim Swaps, Identity theft among other risks to worsen.

Recommendations

1. ***To the consumers, they should understand the costs or charges and associated risks of using a digital service by inquiring from their digital service providers before subscribing to them.*** This can increase their potential of knowing their financial flow such that in case of suspicion of digital theft, they can easily detect it to seek corrective action.
2. ***Bank of Uganda to amplify public awareness campaigns on digital financial fraud literacy.*** For instance educating the public on how to safely connect to, and use the internet while making online transactions. Connections via public Wi-Fi (hotspots such as coffee shops, internet café, hotels among others) when making payments and online banking are not safe as they are susceptible to fraudsters. It is unfortunate that most of the digital users are unaware of such key security concerns that may lead them succumb to digital theft.
3. ***Bank of Uganda in liaison with the Deposit Protection Fund of Uganda, should conduct annual IT Systems Audits at least twice a year for commercial banks, remittance platforms, and telecom companies to assess their level of safety.*** One of the main benefits of systems audit is that it can help combat risks related to availability, integrity, and confidentiality of IT processes and infrastructure.
4. ***The forensic teams of Police, banks, and telecom companies should be reinforced and retooled in a bid to learn new technologies and techniques that hackers use to compromise systems.*** They should also be in position to track digital fraud and identify the perpetrators such that when the perpetrators are tried in courts of law, empirical evidence is available to implicate them.
5. ***Stakeholder collaboration, that is, Bank of Uganda, Uganda Communications Commission, National Identification and Registration Authority, clients, Commercial banks, and telecom companies to liaise with security agencies to render immediate assistance in case of digital fraud.***
6. Bank of Uganda should design an app that is used to report digital fraud with ability to render assistance to the victims. This will also support the maintenance of a database for commonly used forms of digital fraud and hence find possible solutions to eliminate them.

Bank of Uganda should design an app that is used to report digital fraud with ability to render assistance to the victims.

7. Bank of Uganda should engage Policy Think Tanks that can conduct research, find sustainable remedies and new models to safeguard digital financing. Banks and telecom companies should have a department for Think Tank Partnership and Research to identify security measures that protect peoples' money.

8. Banks and telecom companies should invest in technology that addresses emerging security issues in digital finance. **A designated budget for such institutions should be in place every financial year to develop software and technologies that foster financial security also including increasing the budget for digital financial literacy and its associated risks.**

9. The Parliament of Uganda should review The Electronics Transactions Act, 2011 to include an article that directs digital finance service providers to refund proven victims of digital fraud.

10. The government should increase the budget for the Criminal Investigations Department (CID) of the police in order to procure the latest technology. CID officers should be retooled with contemporary skills to track lost most mobile phones and gadgets before SIM cards are swapped by fraudsters as well tracking online fraudsters.

References

1. 2021/2022 Police Report
2. A 2020 report by the Police's Criminal Investigations Directorate (CID)
3. <https://www.bou.or.ug/bou/bouwebsite/PaymentSystems/dataandstat.html>
4. <https://www.upf.go.ug/wp-content/uploads/2023/02/OFFICIAL-ANNUAL-CRIME-REPORT-2022-Web-Version.pdf?x89335>
5. Klaus S (2016) The Fourth Industrial Revolution: World Economic Forum. https://bou.or.ug/bou/export/sites/default/mediacenter/FSS/BOUs-role-in-managing-Digital-financial-risks_.pdf
6. Uganda Bureau Of Statistics, 2022
7. Uganda police force annual crime report 2022
8. World Bank Development Indicators, 2023

CID officers should be retooled with contemporary skills to track lost most mobile phones and gadgets before SIM cards are swapped by fraudsters as well tracking online fraudsters