Technology and Governance Program 13th March 2025

MRPC

The Mashariki Today

Rising Online Fraud in East Africa: An Analysis of Policy Options

Photo credit: techtrendske.co.ke

By Felistus Kandia, MRPC Researcher

Introduction

East Africa is witnessing a rapid digital transformation that promises substantial economic growth and regional integration. The region has become a major hub for technology development, with Kenya, Uganda, and Rwanda leading the charge in mobile banking, digital services, and cross-border trade.[1] However, this growth comes with its own set of challenges, most notably the rise of cybercrime and online fraud. As East Africa embraces the benefits of digital technology, it has also become a prime

[1] East African Community. (2023, February 1). *EAC readies to accelerate regional digital integration with cross-border data flow framework*. East African Community. https://www.eac.int/press-releases/3287-eac-readies-to-accelerate-regional-digital-integration-with-cross-border-data-flow-framework

target for cybercriminals. From mobile money fraud to the hacking of financial institutions, online fraud is increasingly undermining the region's economic progress. The rise of digital fraud is a particular concern for East Africa's burgeoning fintech sector,[2] which relies heavily on secure digital platforms to drive financial inclusion. This article explores the increasing prevalence of online fraud in Kenya, Uganda and Tanzania, examines its economic and social impact, and provides policy recommendations to combat this growing security threat.

The Rise of Digital Identity Fraud in East Africa

East Africa has recently been reported as the region with the highest rejection rates for digital identity verification in Africa.[3] According to the *2025 Digital Identity Fraud in Africa Report* by SmileID, the region recorded a 27% rejection rate, significantly higher than Central and West Africa, which stood at 22%.[4] Rejection of biometric and document verification occurs when there is mismatched or falsified information, which has become increasingly common as fraudsters exploit weak points in digital systems.

One of the most prevalent forms of fraud is *spoofing*, where cybercriminals impersonate trusted sources to deceive individuals into providing sensitive information. These fraudsters often use falsified documents, such as altered national IDs, driver's licenses, and passports, to bypass security checks. National IDs, for instance, were found to have the highest fraud rate in the region at 27%.[5] Financial institutions, particularly those within the fintech sector, have become prime targets, as fraudsters seek to exploit vulnerabilities in their verification processes.

[2] Citizen Digital. (2024, January 25). *East Africa tops continent's digital identity fraud in 2024*. Citizen Digital. https://www.citizen.digital/tech/east-africa-tops-continents-digital-identity-fraud-in-2024-n356776
[3] ibid
[4] SmileID. (2025, February 1). *2025 digital identity fraud in Africa report*. SmileID. https://usesmileid.com/blog/2025-digital-identity-fraud-in-africa-report
[5] Citizen Digital. (2024, January 25). *East Africa tops continent's digital identity fraud in 2024*. Citizen Digital. https://www.citizen.digital/tech/east-africa-tops-continents-digital-identity-fraud-in-2024-n356776

As fraud tactics evolve, fraudsters are using advanced technologies like deep fakes and generative AI to create more convincing fake identities and documents. This technological arms race makes it increasingly difficult for digital security systems to detect fraudulent activities. In countries like Kenya, Uganda, and Rwanda, where mobile money platforms and digital banking are integral to the financial ecosystem, this surge in digital fraud poses a significant risk to economic stability and consumer trust.

The Impact of Cybercrime on East Africa's Financial Institutions

Cybercrime poses a growing threat to the financial institutions across East Africa, with 74% of businesses in the region placing cyber risks at the top of their agenda.[6] With the region's rapid digitalization, banks, fintech platforms, and other financial institutions have become prime targets for cybercriminals. These institutions hold vast sums of money and personal data, making them attractive targets for attackers. For instance, in 2023, Uganda reported a loss of USD 419,486.87 to cybercrime,[7] while on the other hand Kenya lost USD 83 million in 2023, according to the Communications Authority of Kenya.[8]

Photo credit: Africa Defence Forum

[6] PwC Kenya. (n.d.). *East Africa digital trust insights*. PwC. https://www.pwc.com/ke/en/publications/east-africa-digital-trust-insights.html#:~:text=As%20cyber%20threats%20become%20more,agenda%E2%80%94well%20above%20global%20averages.

[7] Business Times Uganda. (2023, December 21). *Shs1.5 billion lost in cyber attacks in 2023*. Business Times Uganda. https://businesstimesug.com/shs1-5-billion-lost-in-cyber-attacks-in-2023/#:~:text=In%202023%20alone%2C%20a%20staggering,the%20report%20reads%20in%20part.

[8] The Star. (2024, October 26). *Kenya lost Sh107.1 billion to cybercrime in 2023, CA reveals*. The Star. https://www.the-star.co.ke/business/kenya/2024-10-26-kenya-lost-sh1071-billion-to-cybercrime-in-2023-ca-reveals?__cf_chl_rt_tk=BYD7E0IraoVUofL5FpoRVr15rmwSjjhct8ZM0ZL30G0-1738581285-1.0.1.1-sn0VYUF6.hlg2EHmkTQiBAV95_o.maTNarQkXhRWgkE

One notable example of a cyberattack in the region occurred when a cybercrime syndicate attempted to hack into Equity Bank, one of the largest financial institutions in East Africa. The syndicate, comprising eight Kenyans, three Rwandans, and a Ugandan, had previously conducted similar attacks in Kenya and Uganda.[9] In response to this growing threat, the Director of Criminal Investigations in Kenya issued warrants for the arrest of 130 suspected hackers and fraudsters involved in banking fraud. In addition, during an operation referred to as Serengeti, INTERPOL, in partnership with 19 African countries worked between 2 September and 31st October 2024, to disrupt cybercrime networks in the continent. In East Africa, and specifically in Kenya, the operation resulted in the officers cracking a case of online credit card fraud linked to losses of USD 8.6 million with ties to foreign actors including Chinese nationals.

These incidents highlight the increasing sophistication of cybercriminals and the rising financial losses from cyber insecurity, which threaten to undermine East Africa's economic growth.

Photo credit: telecomreviewafrica.com

The prevalence of cyberattacks targeting financial institutions underscores the region's vulnerability due to its underdeveloped cybersecurity infrastructure. Despite having established some regulatory measures, East Africa's digital infrastructure is ill-equipped to handle the growing risks of cybercrime due to factors primarily including limited public awareness on cybercrimes, and sophisticated tactics used by cyber criminals.[10] In countries like Kenya, Uganda, and Rwanda, financial institutions are investing heavily in cybersecurity, but cybercriminals are continuously finding new ways to exploit vulnerabilities.

The Economic and Social Consequences of Online Fraud

[9] The East African. (2021, July 07). *Rwanda jails 8 Kenyans in Equity Bank hacking case*. The East African. https://www.theeastafrican.co.ke/tea/business-tech/rwanda-jails-8-kenyans-equity-bank-hacking-case-3463908

[10] Cybercrimes, The Eastern Africa Police Chiefs Cooperation. https://eapcco.org/cybercrimes/#:~:text=The%20following%20factors%20continue%20to,service%20and%20other%20business%20schemes.

The economic consequences of online fraud in East Africa are profound.[11] As digital fraud becomes more prevalent, businesses in the region face increasing financial losses, especially in sectors like e-commerce, mobile banking, and fintech. Financial institutions, in particular, are under immense pressure to safeguard their systems from sophisticated cybercriminals who target customer data and financial resources.

The damage caused by cybercrime extends beyond just the financial sector. As consumers lose trust in digital platforms, they become more hesitant to engage in online transactions. This loss of confidence could significantly slow down the region's digital economy, especially in countries like Kenya, where mobile money has revolutionized financial inclusion. In fact, the threat of cybercrime undermines the very foundation of digital financial inclusion, as vulnerable populations, including low-income individuals and the elderly, are often the primary victims of online fraud.

Photo credit: INTERPOL

Additionally, the rise in fraud is having a social impact, as many victims of cybercrime experience emotional and financial distress. Some fraudsters prey on the most vulnerable populations by offering fake job opportunities or loans, which results in financial loss and a loss of trust in digital services. In a region that depends on digital technologies for socio-economic development, these social consequences pose a serious risk to the future of East Africa's digital economy.

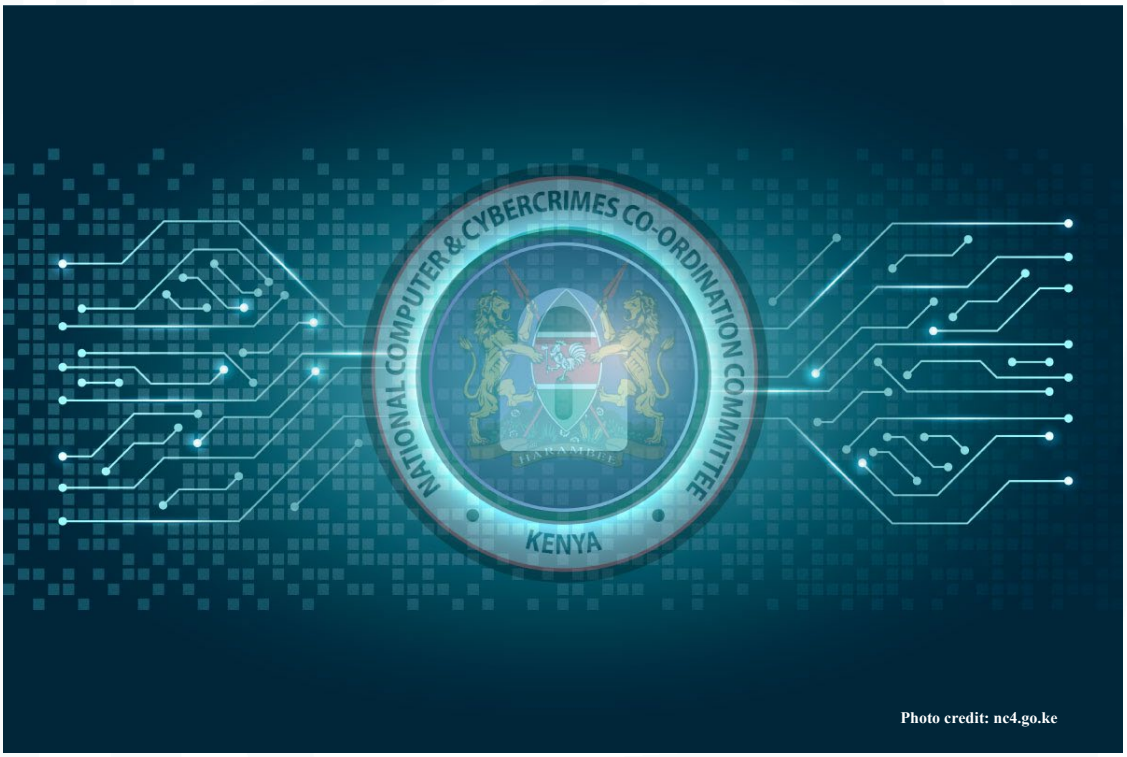
Regional and National Efforts to Combat Cybercrime

Several East African countries are taking steps to address the growing threat of cybercrime. Kenya, Uganda, and Rwanda have all made significant progress in establishing legal frameworks, cybersecurity policies, and response teams to combat

[11] PwC Uganda. (n.d.). *Global economic crime and fraud survey*. PwC. https://www.pwc.com/ug/en/publications/global-economic-crime-and-fraud-survey.html

digital fraud. However, these measures are still in their early stages, and more needs to be done to secure the region's digital economy.

Rwanda has been a regional leader in cybersecurity. In 2015, the country launched a national cybersecurity policy and established a National Computer Security and Response Centre, which detects and responds to cybersecurity threats.[12] Rwanda also passed the *Information and Communication Technology (ICT) Law* in 2016, which criminalizes unauthorized access to data and sets up a framework for managing cybersecurity incidents. The country has also established a National Cyber Contingency Plan to handle cyber crises and passed telecom network security regulations to ensure service providers protect their infrastructure.[13]



Kenya's efforts to address cybersecurity issues began in 2014 with the launch of its National Cybersecurity Strategy.[14] The country also amended its Information and Communications Act to criminalize unauthorized access to computer data.[15] Kenya's

[12] Rwanda Cyber Security and Emergency Response Team. Rwanda Cyber Security and Emergency Response Team. https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245

[13] Digital Watch. (2024, August). *National cybersecurity strategy of the Republic of Rwanda 2024-2029*. Digital Watch. https://dig.watch/resource/national-cybersecurity-strategy-of-the-republic-of-rwanda-2024-2029

[14] Ministry of Interior and Coordination of National Government. (2022). *Kenya cybersecurity strategy*. Ministry of Interior and Coordination of National Government. https://www.interior.go.ke/sites/default/files/2024-05/L-897-KENYA-CYBERSECURITY-STRATEGY-6_220922_103959_220930_161437.pdf

[15] Kenya Information and Communications Act. (n.d.). *Kenya Information and Communications Act*. Kenya Information and Communications Act. https://infotradekenya.go.ke/media/Kenya%20Information%20Communications%20ACT.pdf

National Computer Incident Response Coordination Centre consolidates key cyber infrastructure, and the country has developed regional and international partnerships to combat cybercrime.

Uganda, too, has established laws such as the *Computer Misuse Act* and the *Regulation of Interception of Communications Act* 2011, to protect electronic transactions and information systems.[16] The country also has a National Computer Emergency Response Team, similar to those in Kenya and Rwanda, which monitors and responds to cybersecurity threats. Furthermore, Uganda's National Information Technology Authority provides technical support and cyber training to bolster the country's cybersecurity posture.

Photo credit: theguardian.com

Despite these efforts, East Africa's regional integration in tackling cybercrime is still fragmented. While the African Union's *Convention on Cyber Security and Personal Data Protection* also referred to as the Malabo Convention[17] provides an overarching policy guideline for member states, only Rwanda has signed the convention, leaving other countries, such as Uganda and Kenya, at a disadvantage in terms of regional cooperation and cybersecurity standards.[18] The Convention promotes the establishment of national computer emergency response teams (CERTs) and

[16] Uganda Legal Information Institute. (2011, February 14). *The Computer Misuse Act, 2011*. Uganda Legal Information Institute. https://ulii.org/akn/ug/act/2011/2/eng@2011-02-14

[17] Yohannes Eneyew Ayalew, "The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?" *June 15, 2023*. Retrieved from: https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/

[18] Centre for Intellectual Property and Information Technology Law (CIPIT). (2020, September 15). *The African Union Convention on Cyber Security and Personal Data Protection: Key insights*. CIPIT. https://cipit.org/the-african-union-convention-on-cyber-security-and-personal-data-protection-key-insights/

encourages cooperation between governments and businesses to combat cybercrime. However, to ensure the effectiveness of these measures, more countries in East Africa should sign and implement the convention's provisions.

Conclusion

The rise of online fraud in East Africa is a serious challenge to the region's digital economy. As the region continues to embrace digital technologies, it must also confront the growing threat of cybercrime. While significant strides have been made in enhancing cybersecurity in countries like Kenya, Uganda, and Rwanda, much work remains to be done. By strengthening cybersecurity frameworks, increasing collaboration, and investing in consumer education cantered on increased public awareness, East Africa can better protect its digital economy and ensure that its growing online platforms remain secure, trusted, and resilient to future threats. Only through these concerted efforts can East Africa continue to thrive as a beacon of digital innovation in Africa.

Policy Recommendations

To address the growing threat of online fraud in the region, East African governments must take a multi-pronged approach to cybersecurity to include the following:

1. The first step is to strengthen national and regional cybersecurity frameworks. Governments should prioritize the implementation of the *African Union's Convention on Cyber Security and Personal Data Protection* and ensure closer cooperation between countries in the region to tackle cross-border cybercrime. This would require harmonizing national cybersecurity laws, improving data protection, and establishing national CERTs to respond to incidents effectively.
2. Further, the countries must invest in building robust cybersecurity infrastructures to protect financial institutions and businesses from cyber threats. This includes the adoption of advanced fraud detection systems, enhanced KYC procedures, and

regular security audits to identify and address vulnerabilities. Financial institutions should also work closely with governments and tech providers to develop and implement more secure systems for digital identity verification.

3. Public awareness campaigns are another key aspect of combatting online fraud. Governments and businesses should educate consumers on how to identify phishing attempts, secure their personal data, and protect themselves from fraud. These efforts should focus on vulnerable groups, such as the elderly and low-income individuals, who are often the target of fraudsters.
4. Finally, it is essential to foster regional cooperation and knowledge-sharing between governments, businesses, and law enforcement agencies. As cybercrime increasingly operates across borders, effective coordination is crucial in tracking down fraudsters and bringing them to justice, while this has been done by INTERPOL, through operation Serengeti, more similar programs need to be supported to enhance skills of relevant East Africa law enforcement agencies such as the Eastern Africa Police Chiefs Cooperation Organization (EAPCCO).

Address: P O Box 650 - 00621, Nairobi
Phone: +254 734 088 233 | 0114 088 233
Email: info@masharikirpc.org
www.masharikirpc.org