

Cybercrime in Africa

Chaib Mohamed Toufik¹, Khane Foudil²

¹University of Mohamed khider Biskra, mohamed.chaib@univ-biskra.dz,

²University of Mohamed khider Biskra, foudil.khane@univ-biskra.dz,

Received: 11/08/2024

Accepted: 15/12/2024

Published:19/12/2024

Abstract:

Africa has the fastest internet and phone networks, which are widely used in mobile banking. But this rapid digitization has made the region a target for Cyber-attacks. Criminals are taking advantage of the increasing use of smartphones to steal personal data and Carry out fraudulent operations. The most prominent Cyber blackmail, ransomware, and online fraud such as phishing and hacking into electronic institution emails. The lack of standards governing Cybersecurit Services to great risks.

Keywords: Cyber Crime; threats; Fraud-systems; hacking; Criminal activity; Impact: Data.

Corresponding author: Chaib Mohamed Toufik, e-mail: mohamed.chaib@univ-biskra.dz

1. INTRODUCTION

Cyber Crime or «Computer Crime» appears to have no precise definition. On the one hand, a computer may become the «object» of a crime when theft of a computer hard ware or software occurs. On the other hand, a computer may become the a «subject» of a crime when it is used as an «instrument» to Commit traditional crimes such as fraud, theft, extortion, a new types of criminal activity Such as, denial of service, a Hacks and malware, identity theft, child pornography, or copyright infringement¹

The face of Cybercrime has changed recently, as result of new Internet environments, organized cybercrime groups, and new «Smart» Viruses. The development of new accessible technologies and the expansion of the internet have resulted in new forms of criminal behaviors²

Cybercrime recognizes no borders³. It is unnecessary for the perpetrator in one country may have a direct and immediate effect in anther. This has led to call for speciation to combat There new criminal activities.

I. What is Cybercrime?

The world is waking up to the existing problem of cybercrime with the advancement of technology came great technological innovation in all facets of life that have had a hugely positive impact in these areas, with this advancement came the phenomenon of cybercrime,

Individuals, corporation, organizations and Countries have experienced cyber crime is one from or other. In this day and age, ignorance of what is Cybercrime and its resultant effect could pose a serious Consequences.

Cybercrime in simple terms are Crimes Committed against The Computer or information found on computers or crimes involving Computer and Communication to technologies⁴ of The Cybercrime Convention of the Council of Europe 2001 does not directly define Cybercrime. However, it make provisions for those activities that member states are required to legislate upon these include

- Illegal access - Computer-related forgery
- Illegal interception - Computer-related fraud
- Data interference - Offences related to child pornography
- System interference

II. Types of Cybercrime in Africa

Cybercrime in Africa encompasses a variety. Here are some of the most prevalent types .

1) Business Email Compromise B.E.C

This involves cyber Criminals gaining access to business email accounts to conduct unauthorized transaction or steal sensitive information⁵

2) Phishing

A Hackers use deceptive email or websites to trick individuals into providing personal information such as passwords of credit code number⁵⁻⁶

3) Ransomware

Software that encrypts a victim's data with a Hacker demanding a ransom to restore access⁵⁻⁶

4) Banking Trojans and stealers

These are designed to steal banking credentials and other Sensitive information from users ⁵⁻⁶

5) Online Scams and Extortion

This includes various forms of Fraud, such as romance scams advance fee fraud (419 scams) and digital extortion⁵⁻⁶

6) Crime as a Service

Platforms that provide cyber criminals with tools and services to conduct cyber a Hacks⁵.

There cyber threats are evolving rapidly; posing significant challenges to cyber security efforts accords the continent.

III. Impact of cybercrime on African society

Cybercrime has a profound impact on African society, affecting various aspects of life and development, here are some they points.

1) Economic losses

Cybercrime leads to significant financial losses For instance; Africa experienced a reduction of over 10% in G.A.P. due to cybercrime with an estimated Cost of S4.12 billion in 2021⁷⁻⁸

2) Businesses Disruption

Cyber-attacks disrupt business operations, leading to loss of revenue and trust. In 2017, the business Community lost approximately 3,5\$ billion to cyber fraud and theft.⁹

3) In creased Vulnerability

The rapid adoption of digital technologies without Corresponding cyber security measures has increased Vulnerability this is exacerbated by a gap of law enforcement capabilities to combat cybercrime effectively¹⁰

4) Psychological and social impact

Victims of cybercrime often suffer from psychological distress and social consequences, the loss of personal data and financial resources can lead to emotional and mental health issues¹¹

5) National Security threats

Cybercrime pores a threat to national security by targeting critical infrastructure and government systems. This can lead to disruption in essential Services and undermine public trust in government institutions.

6) Digital Divide

The disparity in cyber security resilience between different region and socioeconomic groups can widen the digital divide, leaving less resilient.

Communities more vulnerable to cyber threats¹¹

Addressing these challenges require a comprehensive approach, including enhancing cyber security law enforcement Capabilities, and raising awareness about cyber threats is there a specific aspect of cybercrime in Africa.

IV. Cyber security measures in Africa

Cyber security in Africa is growing concern as the continent experiences rapid digital transformation. Here are some Key Measures being implemented to enhance cyber security.

1) National Cyber security strategies

Many African Countries are developing implementing National Cyber security strategies to address the increasing Cyber threats. These strategies often include legal, technical, and organizational measures.¹²

2) Capacity building

There is a strong focus on building Cyber security skills and awareness among the population. This includes training programs, Workshop, and awareness Campaigns to educate individuals and organizations about practices.¹³

3) International Cooperation

African Countries are collaborating with international organizations like Interpol and the international Telecommunication Union. (I.T.U) to strengthen their Cyber security Frame works and share threat intelligence.¹²⁻¹⁴

4) Cyber Resilience

Businesses are encouraged to develop Cyber resilience strategies, which involve protecting data integrity, integrating Cyber risk protection into decision-making processes, and ensuring Continuous monitoring and response to cyber threats.¹⁵

5) Legislative Frame works

Efforts are being made to enhance the legislative frame works related to cyber security. This includes updating laws to address new types of cybercrimes and ensuring that there are clear regulation for data protection and privacy¹³

6) Public-private partnerships

Collaboration between the public and private sectors is crucial for effective Cyber security, Governments and private Companies are working together to share information, resources, and best practices to combat cyber threats.¹⁶

These measures are essential for creating a secure digital environment in Africa, protecting critical infrastructure, and ensuring the safety of individuals and businesses online.

V. Government initiation in Africa about cybercrime

African governments, in collaboration with international organizations, have been actively working to combat cybercrime here some key initiatives.

1) Interpol's African

Cybercrime Operation Desk Funded by the UK foreign, common wealth and development office. This desk specializes in gathering and analyzing information on cybercriminal activity, carrying out intelligence operations and supporting member countries in their fight against cybercrime.¹⁷

2) African Union's Convention on Cyber security and personal Data protection (Malabo Convention)

This Convention aims to establish a legal framework for cyber security and data protection in Africa; it encourages member states to adopt national Cyber security policies and strategies.¹⁸

3) Regional Cyber security strategies

Various regions within Africa have developed their own cyber security strategies. For example, the East African Community (EAC) has Cyber security strategy that focuses on enhancing regional cooperation and building capacity to tackle cyber threats.¹⁹

4) Capacity building and training

Many African Countries are investing in Capacity Building and training for law enforcement and other stakeholders. This includes

workshops, Seminars, and training programs to enhance skills, and knowledge in cyber security.²⁰

5) Public Awareness Campaigns

Government and organization are also running Public awareness Campaigns to educate citizens about the risks of cybercrime and how to protect themselves online.²¹

These initiatives are Crucial in addressing the growing threat of cybercrime in Africa and ensuring a Suffer digital environment for all.

VI. Cybercrime legislation in Africa

1) African Union Convention on cyber security and personal Data protection

In 2014, the African Union (AU) adopted the African Union Convention on cyber security and personal Data protection. This convention aims to establish legal Framework for cyber security and personal data protection across member states.²²

It embodies existing Commitments at sub-regional and international levels to build the information Society.

The Convention, addresses gas related to legal recognition of data Communication, electronic Signatures, consumer protection, intellectual property rights.

2) Guide line for a Model Cyber security law

The guideline for a Model cyber security law in African Union Member states provides guidance Cyber security legislation. It explains key features and benefits of a standard cyber security law.²³

While not binding, it offers guiding principles for African states to establish standards for ensuring cyber security or cybercrime law. It emphasizes respect for human rights, law enforcement standards, and judicial processes.

3) Current landscape

Approximately 29 out of 54 African Countries have introduced specific cyber security legislation, according to the Global Cyber Security Index (2021)²⁴

However, there's room for improvement, and more concerted efforts are needed to address cyber threats effectively.

Remember that Cyber security is crucial for Africa's digital transformation. Strengthening legislation, cooperation, and Capacity-building will contribute to a safer digital environment. It have further questions feel free to ask

Conclusion

Cybercrime that uses Computers to commit other crime may involve using Computers or networks to spread malware, illegal information or illegal images. Cybercrime are often doing both at once.

They may target Computers with viruses first and then use them to spread malware to other machines or throughout a network.

Cybercrime in Africa is an evolving challenge that warrants attention. With over 500 million internet immense growth potential, but also increased Vulnerability to cyber threats.²⁵

Africa must prioritize Cyber security measures, faster collaboration, and stay vigilant to mitigate the impact of cyber threats in its societies and economies.

List of references:

- ¹ See s Brenner & L L Clarke, Distributed Security: Preventing Cybercrime,(2005) John Marshall Journal of Computer and Information Law 659-709 at 665-666 and s Brenner & BJ Koops. “Approaches to jurisdiction (2004) journal of High Technology law 1-46 at 7. It should be noted that the terms «computer crime» «Cybercrime» and cit crime”
- ² S Brenner Cybercrime Investigation and Prosecution: the Role of Penal and procedural Law 2001 Murdoch University Electronic Journal of Law 1-16
- ³ See MD Goodman & s Brenner “The emerging Consensus or Criminal Conduct in cyberspace” 2002 International Journal of law and Information Technology 139-223 at -142, 146-150
- ⁴ W Jayawickrama, Cyber Crime – Threats, Trends and Challenges, Computer Security Week 2002 – Brisbane, 3
- ⁵ The International Criminal Police Organization (<https://www.interpol.int>).
- ⁶ International development aid and economic and humanitarian assistance stakeholders (<https://www.developmentaid.org>)
- ⁷ <https://link.springer.com>
- ⁸ <https://info.arxiv.org>
- ⁹ Africa center for strategic studies (<https://africacenter.org/>)
- ¹⁰ The International Criminal Police Organization (<https://www.interpol.int>).
- ¹¹ The International Criminal Police Organization (<https://www.interpol.int>).
- ¹² The International Criminal Police Organization (<https://www.interpol.int>).
- ¹³ Ptsecurity.com ([https:// www.ptsecurity.com](https://www.ptsecurity.com))
- ¹⁴ International Telecommunication Union (<https://www.itu.int>)

¹⁵ The Brookings Institution (<https://www.brookings.edu>)

¹⁶ <https://link.springer.com>

¹⁷ The International Criminal Police Organization (<https://www.interpol.int>).

¹⁸ The International Criminal Police Organization (<https://www.interpol.int>).

¹⁹ The International Criminal Police Organization (<https://www.interpol.int>).

²⁰ The International Criminal Police Organization (<https://www.interpol.int>).

²¹ Kampala International University (<https://kiu.ac.ug>)

²² African Union web site (<https://au.int>)

²³ The Knowledge Portal for Cyber Capacity Building
(<https://cybilportal.org>)

²⁴ The World Economic Forum (<https://www.weforum.org>)

²⁵ leading African law firms (<https://lexafrica.com>)