# AFRICA CYBER THREAT REPORT
# 2025

# TABLE OF
# CONTENTS

# THREAT LANDSCAPE: AN OVERVIEW

## Current State of Cyber Threats

### FREQUENCY OF ATTACKS:

## 2,164

In 2024, African organizations faced an average of 2,164 cyberattacks per week, a 23% increase from 2023.

### FINANCIAL IMPACT:

## $4 billion

Africa's annual financial losses to cybercrime, affecting businesses, governments, and individuals.

### KEY SECTORS TARGETED:

**Banking**, **telecommunications**, and **public services** are among the most affected industries, with mobile money platforms being a prime target.

## Geographic Hotspots

**Nigeria**: As one of Africa's largest economies, Nigeria faces sophisticated cyber threats, including phishing, ransomware, and fraud.

**South Africa**: With advanced financial systems, South Africa experiences high levels of targeted attacks on banking and e-commerce platforms.

**Kenya**: The growth of mobile money services like M-Pesa has made Kenya a hotspot for mobile fraud and SIM-swapping attacks.

# CYBERCRIMINAL TACTICS AND TECHNIQUES

## Common Tactics

**1**

### Phishing Attacks:
Phishing remains a leading threat, with 67% of African businesses reporting successful phishing attempts in 2023

**2**

### Ransomware:
Cybercriminals encrypt critical systems and demand payment, often in cryptocurrency, crippling businesses and government operations.

**3**

### Mobile Money Fraud:
Mobile platforms are frequently exploited through social engineering, insider threats, and weak authentication mechanisms.
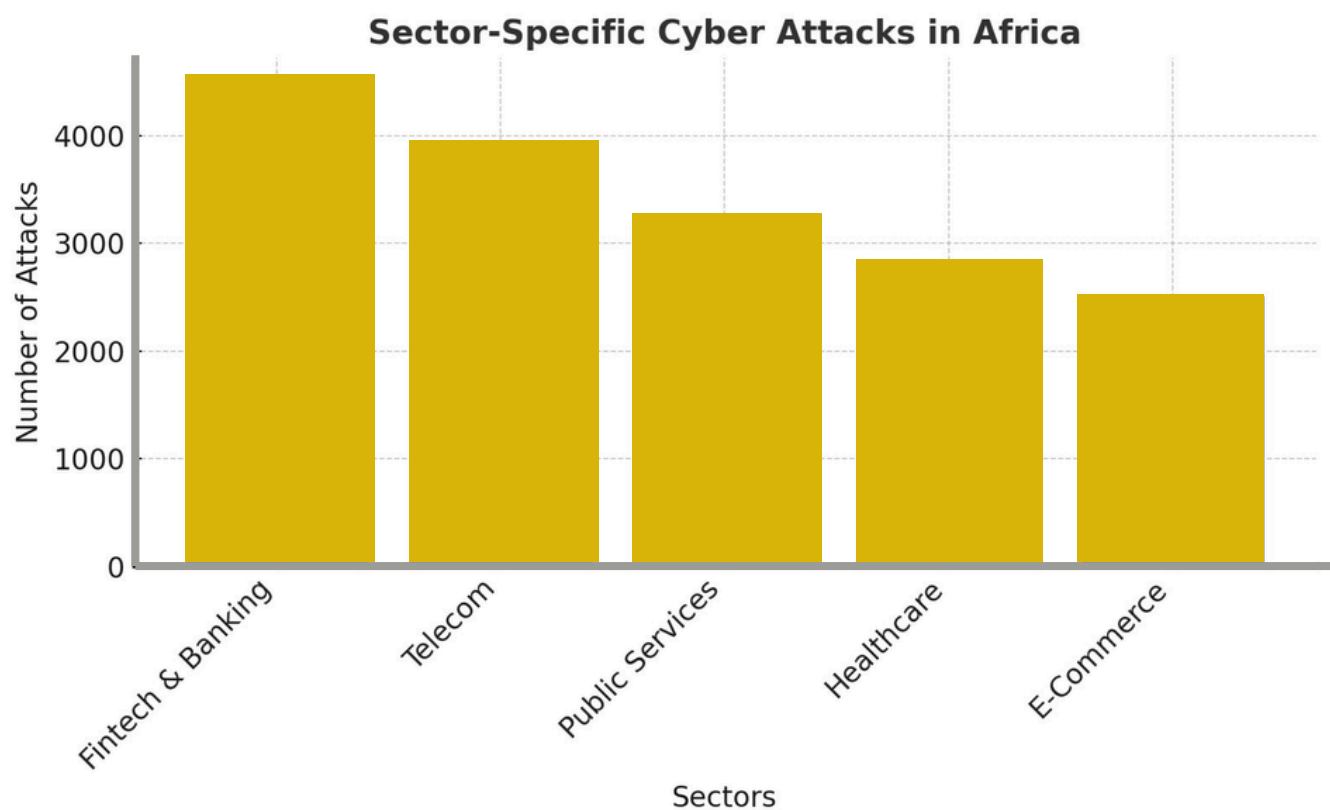
## Emerging Trends

**AI-Driven Attacks:** Cybercriminals are increasingly leveraging AI to enhance phishing campaigns and automate large-scale attacks.

**Targeted Cyber Espionage:** Advanced Persistent Threat (APT) groups are focusing on African governments and critical infrastructure.

# SECTOR-SPECIFIC INSIGHTS



Sector-Specific Cyber Attacks in Africa

# KEY CHALLENGES

## Fragmented Regulations:

Only 30 out of 54 African countries have enacted cybersecurity laws, creating gaps for cybercriminals to exploit.

## Human Vulnerabilities:

A significant lack of cybersecurity awareness and training among employees.

## Resource Constraints:

Limited budgets for cybersecurity in both the public and private sectors.

## Technology Gaps:

Absence of advanced threat detection systems and real-time monitoring.

# OPPORTUNITIES FOR AFRICA

## Leveraging Public-Private Partnerships:

Collaboration between governments, businesses, and international organizations can pool resources and expertise to address systemic vulnerabilities.

## Building Local Talent:

Investing in cybersecurity education and training can create a skilled workforce capable of tackling emerging threats.

## Harnessing Innovation:

Africa's burgeoning tech ecosystem can drive the development of innovative cybersecurity solutions tailored to the continent's unique challenges.

## Regional Collaboration

Harmonized regulations and shared intelligence can strengthen Africa's collective defense against cyber threats.

# RECOMMENDATIONS

## Harmonize Policies:

Develop unified cybersecurity frameworks across African countries to close legislative gaps.

## Building Local Talent:

Allocate resources to advanced cybersecurity technologies, such as AI-driven threat detection.

## Promote Awareness:

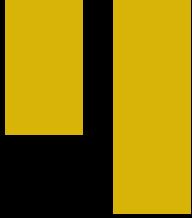Launch continent-wide education campaigns to improve cybersecurity literacy.

## Foster Collaboration:

Establish regional cybersecurity centers to facilitate information sharing and coordinated responses.

## Encourage Research and Development:

Support the growth of local cybersecurity startups and innovation hubs.

# FUTURE PROJECTIONS

## $700 BILLION

The expected contribution of the digital economy to the continent's GDP by 2030. However, achieving this potential requires a secure digital foundation. Without immediate and sustained action, cyber threats could undermine Africa's progress and erode trust in its digital systems.

# A CALL TO ACTION

Africa's digital transformation presents an unprecedented opportunity for growth, but it also exposes critical vulnerabilities. At Cyber Future Africa, we believe that securing Africa's digital future requires more than just technological solutions—it demands leadership, expertise, and unwavering commitment.

Our team comprises global cybersecurity elite experts with years of experience tackling some of the world's most sophisticated cyber challenges. Coupled with the deep understanding and leadership of our native African team, we bring a unique combination of local insight and global excellence. This dual perspective allows us to address Africa's cybersecurity needs with precision and impact.

Cyber Future Africa is dedicated to:

- **Building Awareness:** Through targeted campaigns and educational initiatives, we empower organizations and individuals to identify and mitigate cyber threats.

- **Providing Expertise:** From conducting comprehensive risk assessments to designing robust cybersecurity frameworks, we deliver solutions tailored to Africa's evolving landscape.

- **Driving Innovation:** We support local talent and partner with innovation hubs to develop cutting-edge tools and strategies that anticipate emerging threats.

- **Advocating for Policy Change:** We work closely with policymakers to harmonize regulations, foster regional collaboration, and create a unified defense against cybercrime.

Cybersecurity is not just a technical challenge—it's a shared responsibility. Whether you're a government official, a business leader, or an everyday user, you have a role to play in securing Africa's digital ecosystem.

# WORK WITH US

Join us in making a difference. Together, we can turn challenges into opportunities and ensure that Africa thrives in the digital age. Reach out to Cyber Future Africa today to learn how we can help secure your digital future.

**Cyberfutureafrica** ™

● PROTECTING AFRICA

971-330-4208

www.cyberfutureafrica.com
info@cyberfutureafrica.com

110 N Akard Street
Dallas, TX 75201