FNA GROUP

African Cybersecurity Report 2026

FNA Group — Annual synthesis of the continent's cyber threat landscape

Executive summary

Africa's digital expansion has unlocked extraordinary economic opportunity — and an equally fast-growing exposure to cyber risk.

In 2026, the threats that matter most are no longer abstract: ransomware against critical infrastructure, commercial spyware on the mobile devices of decision-makers, financial fraud across mobile-money rails, and espionage tied to electoral and geopolitical pressure.

Key findings

1. Risk is concentrating in critical services. Energy, telecoms, banking and government remain the highest-value targets.

2. Mobile is the primary battleground. Spyware, malicious apps and SIM-swap fraud exploit the device leaders and citizens depend on.

3. Intelligence beats remediation. Continuous cyber threat intelligence contains campaigns earlier and far more cheaply than recovery.

The threat landscape

The African cyber threat landscape: connectivity outpaces defensive maturity, widening the attack surface across mobile-first economies.

Ransomware and extortion: double-extortion is now the default against institutions where downtime is intolerable.

Mobile spyware and surveillance: traditional endpoint controls fall short on mobile, the sharpest edge of risk for high-value individuals.

State-aligned espionage: election cycles and geopolitical competition draw sophisticated actors toward government networks.

Request a briefing

FNA Group delivers intelligence and cybersecurity programmes tailored by sector and threat exposure. Contact us at https://fnagroup.africa/contact to arrange a confidential briefing.