ZIMSWITCH
Cyber Security Bulletin



CyberSmart: Navigating Risk in a Connected World

As Africa's digital growth accelerates, so do the risks of cyber threats. This bulletin highlights the challenges of our increasingly connected world, the real dangers we face, and how institutions can be proactive to protect themselves.

Are We Secure Enough?

Increased connectivity across the continent has unlocked unprecedented innovation. But with growth comes vulnerability. From phishing scams to ransomware targeting financial systems, banks must fortify their digital assets to stay ahead of evolving threats.

A CASE STUDY OF AFRICA

Africa: Rapid Growth, Rising Risks

High Attack Rates: Threat reports reveal that African organizations face 3,000–4,700 cyberattacks weekly, far exceeding global averages.

Primary Targets: Finance, telecoms, government, and healthcare sectors are hit hardest. Notably, Nigeria ranks third globally in ransomware attacks, with 3,459 detections in 2024 alone.

Recent Cyber Attacks in Africa

1. Telecom Namibia (Dec 2024):
Leaked 626 GB of customer data after a ransomware attack.

2. Electricity Company of Ghana (Mar 2024):
Operations were down for a week due to ransomware, causing losses between GH¢400–500 million (US$34–42 million).

3. South Africa's National Health Laboratory Service(Jun2024)
Ransomware crippled lab diagnostics at 256 healthcare facilities, disrupting critical services.

4. Uganda Telecoms (Feb 2024):
DDoS (distributed denial of service) attacks by Anonymous Sudan targeted MTN and Airtel over political issues.

5. Nigeria's Flutterwave (Apr 2024):
Flutterwave experienced a cyber security breach, which allowed cyber criminals to divert₦11 billion to various bank accounts.

This shows Africa is at risk and so vulnerable that it's a testing ground for cyber criminals, hence the need to know how to protect yourself. There are basic things to know and below are some of them:

Social Engineering: A Growing Threat

What is Social Engineering?
It is a tactic used by attackers or cyber criminals to exploit human psychology and trick victims into sharing sensitive information. Common methods include phishing emails, phone scams, QR code fraud, and impersonation.

Red Flags to Watch For:

- Unexpected requests marked as urgent or confidential.
- Emails with unverified sender details, odd domains, or mismatched phone numbers.
- Emotional manipulation tactics like "Your account will be frozen!"
- Suspicious attachments or files, especially .exe documents.
- QR codes that direct you to unfamiliar sites.
- Requests for credentials or OTPs (One-Time Passwords) via phone or SMS.

Ransomware Attacks
Ransomware attacks are a type of cybercrime where malicious software called ransomware infects a computer or network, encrypts files or locks access, and then demands a ransom payment to restore access.

AI-Powered Attacks
Cybercriminals use artificial intelligence to automate phishing, generate deepfakes, and bypass traditional security systems. AI can mimic user behavior, making detection harder

Protecting today means less repairing tomorrow

- Implement a Risk-Based Cybersecurity Framework
- Align cybersecurity with enterprise risk management (ERM) to prioritize threats based on impact and likelihood
- Strengthen Human-Centric Defenses
- Members are encouraged to conduct regular staff training on phishing, social engineering, and insider threats
- Secure Critical Infrastructure and Applications
- Harden systems like ATMs, mobile banking apps, and payment gateways i,e enable Enable 2FA (two-factor authentication) on all banking apps, Keeping your bank applications updated to avoid vulnerabilities.
- Perform regular vulnerability assessments and penetration testing
- Ensure Regulatory Compliance and Data Governance
- Comply with standards like PCI-DSS, GDPR, and local banking regulation.

Zimswitch attested to PCIDSS Compliance in line with International Standards. Members with need for training are required to contact us on **marketing@zimswitch.co.zw**

Final Thoughts

Africa's digital boom brings incredible opportunities, but it also attracts rising cyber threats. Real-world incidents, ranging from telecom disruptions to healthcare crises, highlight the need for vigilance.

Remember:

Phishing accounts for 34% of cyber activity in Africa.

Be cautious with urgent requests, verify suspicious communications, and consistently update your security safeguards.

Zimswitch: we connect, we secure, we thrive.
Stay Connected and Stay Protected.