UNIX Trainers & Consultants
Head Office: Wema Twins Annex, Plot No. 181,
Boko-Bagamoyo Road, P.O. Box 33826, Dar es salaam.
Mob: +255-715-361-880/+255-754-361-880
Email: info@unixtrainers.com; training@unixtrainers.com
Website: www.unixtrainers.com

Essential Knowledge and Skills on the Implementation of Cybersecurity in the Public Sector

Course Overview

The **"Cybersecurity Essentials for African Public Stewardship"** is a 5-day intensive program designed to transform civil servants from "potential vulnerabilities" into "digital defenders." Recognizing that **90% of cyber breaches involve human error**, this course focuses on practical, low-cost, and high-impact security measures. It covers the geopolitical context of cyber-warfare in Africa, the legal requirements for data protection (e.g., GDPR-aligned local laws), and the technical essentials of securing government devices and networks.

Program Objectives

By the end of this program, participants will be able to:

- **Identify** the most common cyber-threats targeting African governments (Phishing, Ransomware, and Social Engineering).
- **Implement** essential "Cyber Hygiene" practices for personal and departmental devices.
- **Navigate** the legal obligations under National Data Protection Acts and the AU Malabo Convention.
- **Respond** effectively to a security breach using a structured Incident Response Framework.
- **Advocate** for a "Security-First" culture within their respective Ministries, Departments, and Agencies (MDAs).

Course Coverage (Modules)

Day 1: The Cyber Landscape & Geopolitics in Africa

- **Cybersecurity in Africa:** Analyzing the rise of mobile-based attacks and state-sponsored espionage.
- **The Malabo Convention:** Understanding the continental framework for cybersecurity and data protection.
- **Digital Sovereignty:** Why protecting government data is a matter of national security.

Day 2: The Art of Digital Defense (Cyber Hygiene)

- **Password Mastery & MFA:** Moving beyond simple passwords to Multi-Factor Authentication (MFA).
- **Safe Browsing & Remote Work:** Securing home offices and public Wi-Fi usage for government officials.
- **Device Hardening:** Practical steps for securing smartphones, tablets, and laptops.

Day 3: Combating Social Engineering & Phishing

- **The Psychology of the Attack:** How hackers use "Urgency" and "Authority" to trick officials.
- **Spotting the Bait:** A practical workshop on identifying spear-phishing emails and malicious links.
- **Physical Security:** Managing the risks of "lost" USB drives and unauthorized office access.

Day 4: Data Privacy & Legal Compliance

- **Data Classification:** Identifying what is Public, Internal, Secret, and Top Secret.
- **Legal Responsibilities:** Understanding personal and institutional liability under local Data Protection laws.
- **Cloud Security:** Securely using shared government digital infrastructure (e.g., SITA in South Africa or e-GA in Tanzania).

Day 5: Incident Response & Action Planning

- **The "Kill Chain":** Understanding how a cyber-attack unfolds and where to stop it.
- **Reporting Protocols:** Who to contact when a breach is suspected (The Role of the National CERT/CSIRT).
- **Action Planning:** Developing a "Cyber-Security Awareness Plan" for the participant's home department.

Target Participants

- **Senior Management & Directors:** To understand the strategic and legal risks.
- **Administrative & Executive Officers:** To master daily digital hygiene.
- **ICT Support Staff:** To align their technical support with global security standards.
- **Legal & Human Resource Officers:** To manage data privacy and employee security policies.
- **Public Relations Officers:** To handle communication during a cyber-incident.

Expected Outputs

Participants will graduate with a **"Cyber Defence Portfolio"** containing:

- **A Personal Cyber-Hygiene Audit:** A completed assessment of their current digital habits and a plan for improvement.
- **A Departmental "Red Flag" Guide:** A one-page visual aid to help colleagues spot phishing and social engineering.
- **An Incident Reporting Flowchart:** A step-by-step guide on what to do in the first 60 minutes of a suspected breach.
- **A Security Policy Memo:** A draft proposal for a "Clean Desk and Clear Screen" policy for their office

---

©2026 UNIX Trainers and Consultants . All rights reserved.