



# Cybersecurity Essentials

---

OFFICIAL ACADEMIC PROSPECTUS & CURRICULUM GUIDE

**NQF Level:** Industry Certification | **Credits:** N/A

**Delivery:** Online

**Print Date:** April 20, 2026

*Computer generated document*

## PROGRAMME OVERVIEW

PROGRAMME DURATION	6 Weeks
ACADEMIC LEVEL	Industry Certification
TOTAL CREDITS	N/A
SAQA REGISTRATION	Pending
MODE OF DELIVERY	Online
TOTAL INVESTMENT	<b>R 6,500</b> (Registration Deposit: R 799)

### Executive Introduction

In 2026, security is no longer just an IT department issue; it is a fundamental human survival skill in the digital age. Our Cybersecurity Essentials programme is designed to turn you into a 'Hardened Participant' in the modern economy. We move far beyond basic passwords to explore the manipulative psychology of phishing, the mechanics of ransomware, and the strict protocols of data protection that keep individuals and massive companies safe from catastrophic harm.

Participants will deeply explore the 'Modern Threat Landscape,' learning how to identify sophisticated social engineering attacks, secure their digital identities, and implement safe remote-work practices. The curriculum emphasizes 'Personal and Professional Hygiene,' teaching you the specific, daily habits that prevent 90% of all successful cyber-attacks. We focus on the 'Common Sense' of the digital age—ensuring you are the strongest link in the security chain.

This track is the absolutely mandatory foundation for any career in the modern, connected world. By the end of the course, you will possess the critical security literacy required to protect your personal financial information and act as a vigilant, defensive asset to your employer. You will graduate with the confidence to navigate the internet securely, knowing you have the specific knowledge to thwart modern threat actors.

## PURPOSE OF THE LEARNING PROGRAMME

---

To provide foundational 'Security Literacy' for the entire modern workforce. The primary purpose is to ensure that every individual understands the severe risks of the digital world and possesses the practical skills to protect themselves.

To drastically reduce the success rate of common cyber-attacks within organizations. We aim to train 'Security-Aware' employees who can identify and report threats like phishing and social engineering long before they escalate into network breaches.

To promote highly ethical and safe digital participation in the global community. The objective is to produce graduates who understand the profound importance of data privacy laws and organizational security policies, fostering a strict culture of compliance.

To serve as the essential, unshakeable starting point for all specialized cybersecurity careers. This track provides the conceptual grounding required for those who want to eventually move into Ethical Hacking, Security Engineering, or SOC Operations.

To protect the digital integrity of our local and global communities. By training individuals in basic, proactive security protocols, we are contributing heavily to the safety and resilience of our national digital infrastructures against malicious external threats.

## MODULE BREAKDOWN

### **Module 00: Orientation & Student Portal Onboarding**

Mandatory setup: Email, Portal, Labs & PoE guidelines.

### **Module 01: Cyber Threat Landscape Overview**

Comprehensive mastery and practical application of cyber threat landscape overview aligning with industry standards.

### **Module 02: Password Hygiene & Authentication**

Comprehensive mastery and practical application of password hygiene & authentication aligning with industry standards.

### **Module 03: Phishing & Social Engineering Defense**

Comprehensive mastery and practical application of phishing & social engineering defense aligning with industry standards.

### **Module 04: Safe Browsing & Email Practices**

Comprehensive mastery and practical application of safe browsing & email practices aligning with industry standards.

### **Module 05: Data Privacy Basics**

Comprehensive mastery and practical application of data privacy basics aligning with industry standards.

### **Module 06: Assessment: Security Awareness Quiz**

Comprehensive mastery and practical application of assessment: security awareness quiz aligning with industry standards.

# PRACTICAL LAB ENVIRONMENTS

---

This programme includes intensive hands-on practical labs designed to bridge the gap between theoretical knowledge and real-world industrial application.

## Lab 1: Threat Landscape Mapping

Identify common threats using MITRE ATT&CK. Deliverable: Threat matrix + mitigation mapping.

## Lab 2: Password & Authentication Lab

Test password strength and implement MFA. Deliverable: Password policy + MFA setup guide.

## Lab 3: Phishing Simulation & Awareness

Create and test a phishing email (ethical). Deliverable: Phishing test report + training tips.

## Lab 4: Personal Security Hardening

Secure a personal device using best practices. Deliverable: Hardening checklist + before/after scan.

## CAREER FIELDS & OPPORTUNITIES

---

Graduates of this learning programme are aggressively equipped with the specialized competencies required to pursue the following elite professional roles within the global industry:

<b>JUNIOR CYBERSECURITY ANALYST</b>	Advance your career as a Junior Cybersecurity Analyst in the industry.
<b>SECURITY AWARENESS TRAINER</b>	Advance your career as a Security Awareness Trainer in the industry.
<b>IT SECURITY SUPPORT</b>	Advance your career as a IT Security Support in the industry.
<b>RISK ASSESSMENT ASSISTANT</b>	Advance your career as a Risk Assessment Assistant in the industry.
<b>BASIC THREAT ANALYST</b>	Advance your career as a Basic Threat Analyst in the industry.
<b>SECURITY POLICY COORDINATOR</b>	Advance your career as a Security Policy Coordinator in the industry.
<b>ENDPOINT PROTECTION TECHNICIAN</b>	Advance your career as a Endpoint Protection Technician in the industry.

## NEXT STEPS & APPLICATION

Ready to definitively advance your professional trajectory? Formal applications are currently open for the upcoming academic cycle. To securely guarantee your placement in the next intake for **Cybersecurity Essentials**, please complete our online application process or contact our admissions advisory team directly.

### CONTACT ADMISSIONS

**Official Email:** [apply@softkingsacademy.co.za](mailto:apply@softkingsacademy.co.za)

**Academy Website:** [www.skacademy.co.za](http://www.skacademy.co.za)

**WhatsApp:** +27 69 271 9901

**Tel:** +27 21 1097 366 | +27 12 004 3732 | +27 70 5422 373

### DIGITAL STUDENT PORTALS

**Studentzone:** [portal.skacademy.co.za](http://portal.skacademy.co.za)

**Exam Centre:** [exams.skacademy.co.za](http://exams.skacademy.co.za)

**Verify Certificate:** [skacademy.co.za/verify-certificate](http://skacademy.co.za/verify-certificate)

**APPLY ONLINE NOW**