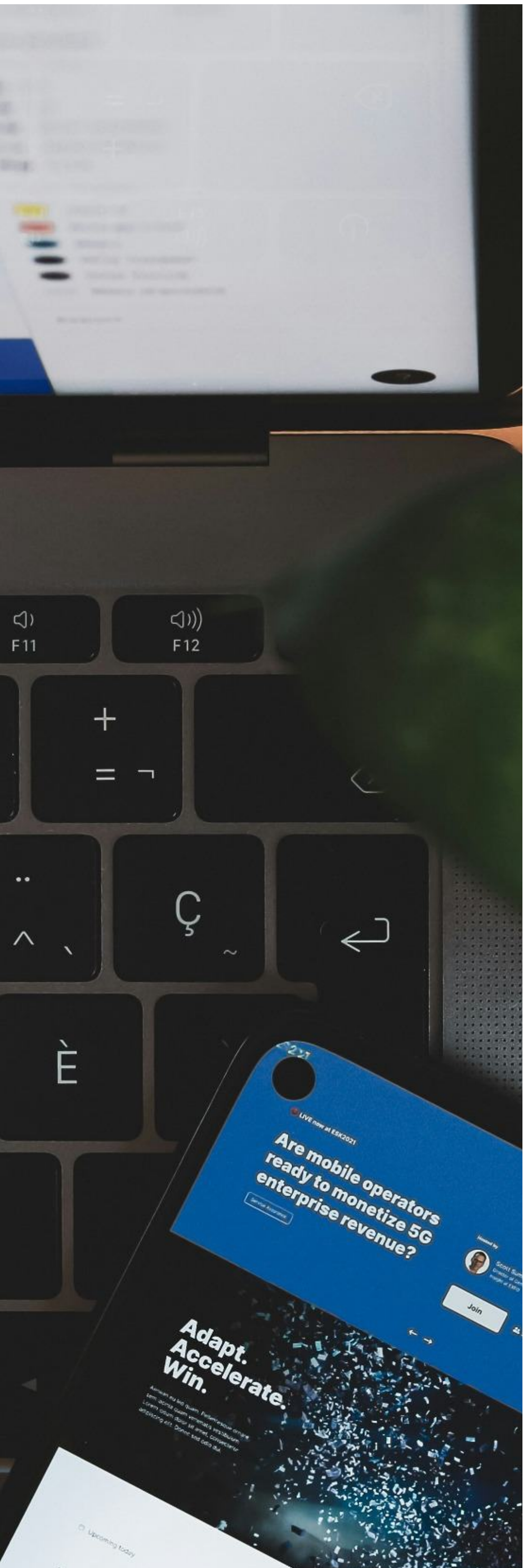
Cyber Security

Cyber Security

Embark on a journey of exploration and innovation with our comprehensive Cyber security Course. Guided by seasoned professionals with extensive field experience, our curriculum blends theoretical knowledge with hands-on exercises, providing a holistic understanding of cyber security principles and practices.

From threat analysis and risk assessment to penetration testing and incident response, you'll delve into every facet of securing digital systems. What distinguishes our course is its focus on real-world scenarios. Through immersive projects and practical case studies, you'll tackle diverse security challenges, sharpen your problem-solving abilities, and develop a vigilant eye for vulnerabilities.

By program completion, you'll emerge as a proficient cyber security analyst, equipped to safeguard critical information and defend against cyber threats. Join us and unlock your potential as a cyber security guardian. Let's fortify digital landscapes together!"

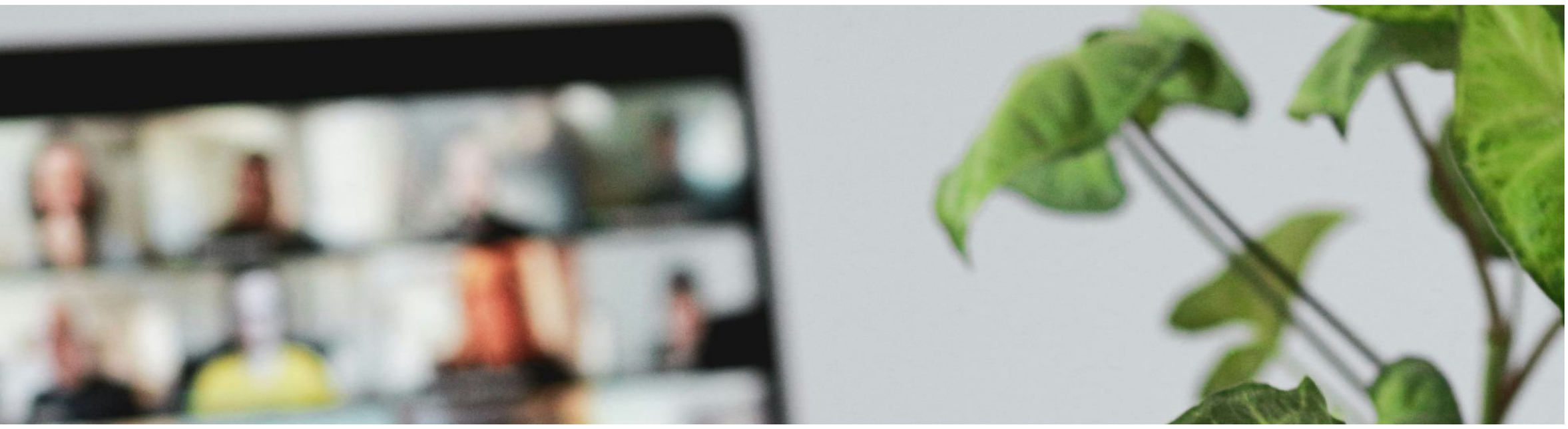


Learning Outcome

- Develop robust end-point protection and network security systems
- Identify cyber threats
- Incident Response to Cyber Attacks
- Design Cyber security controls to protect your organisation
- Investigating data breaches, cyber attacks
- Fundamentals of Cryptography, Cloud Security and Networking

MONTH

August



Who should attend?

- Graduate and Early Career Professionals
- Professionals from the technology and IT fields
- Security analysts
- Professionals Information security officers
- Cyber security consultants
- Executives and business leaders
- Business and Risk management professionals
- Management Compliance officers
- Employees at all levels
- End Users
- Human resources personnel
- Healthcare Professionals
- Law Enforcement and Legal Professionals

MONTH

August

WEEK 1

1. Introduction to Cyber security
2. Components of Cyber security
3. History of cyber security
4. Job Role
5. Cyber security Concepts
6. Fundamental Security Terminology

WEEK 2

1. Basic Networking Concepts
2. Introduction to Networking
3. Network Security Fundamentals
4. The OSI Model
5. Networking devices
6. Types of networking devices
7. IP address and Sub-netting
8. Network attacks and vulnerabilities

WEEK 3

1. Fundamentals of Cryptography
2. Basic terminology
3. Understanding the encryption process
4. Application of Cryptography in Cyber security Security
5. SSL and TLS- What they do and how it works

MONTH

August

WEEK 4

1. Operating System Security
2. Key components of OS security
3. Threats to OS security
4. Types of OS(WINDOWS, MAC , LINUX)
5. Features of different OS
6. Best practices for securing different OS
7. Managing user accounts
8. Why manage user account

MONTH

September

WEEK 5

1. Web Security Basics
2. Common web attack
3. Defending against web attacks
4. Best practices for web security
5. Real-life impact of web attack

WEEK 6

1. Cyber Hygiene and Best Practices
2. Types of password attack
3. Password Management
4. MFA's- common MFA' method
5. Implementing MFA on all accounts
6. Safe Browsing and Email Practices

WEEK 7

1. Introduction to Cyber security Tools
2. Antivirus and Anti-malware
3. Introduction to Security Scanning Tool
4. Intrusion Detection Systems (IDS)
5. Security Information and Event Management (SIEM) Security
6. Project on SIEM
7. Threats And Vulnerability Analysis
8. Threat Landscape

MONTH

September

WEEK 7

9. Vulnerability Assessment
10. Project on VAPT
11. Incidence Response And Handling
12. Incidence Response Framework
13. Digital Forensic Basics
14. Security Operations and Monitoring
15. Log management

WEEK 8

1. Mobile Security Basics
2. Mobile Device Management (MDM)
3. Knowing What MDM can manage
4. Knowing What MDM Solutions Can Do
5. Implementing MDM solutions
6. Bring-your-own-device(BYOD) policies
7. Advantages of BYOD
8. Challenges of BYOD
9. BYOD security best practices
10. Implementing BYOD

MONTH

September

WEEK 8

11. Cyber security Awareness and Training
12. Employee Training Program
13. Key findings
14. Social engineering
15. Common types and attacks
16. Why social engineering is effective
17. Recognising social engineering attacks
18. Implementing effective employee training
19. Key components of cyber security awareness
20. Practice spotting fishing email
21. Defending against fishing
22. Real-life scenario of fishing
23. Cyber security best practices

COST OF PROGRAM PACKAGES

CYBERSECURITY

Class Duration- 2 Month

Prices

- Virtual: ₦120,000
- Physical: ₦150,000