Cybersecurity Awareness for Labour Organizations Training Course

Professional Development Training Course Outline

Category	Trade Unions	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s hyperconnected digital economy, labour organizations, trade unions, worker associations, and employee representative bodies are increasingly targeted by sophisticated cyberattacks, including phishing, ransomware, social engineering, data breaches, and identity theft. Labour organizations manage highly sensitive information such as worker records, payroll data, legal documents, collective bargaining agreements, confidential communications, and financial transactions, making them attractive targets for cybercriminals. As organizations adopt cloud computing, remote work platforms, mobile collaboration tools, and digital communication systems, the need for advanced cybersecurity awareness, data privacy protection, and cyber risk management has become critical for organizational resilience and operational continuity.

Cybersecurity Awareness for Labour Organizations Training Course equips labour organizations with practical knowledge, modern cybersecurity skills, and proactive defense strategies to identify, prevent, and respond to evolving cyber threats. Participants will gain hands-on understanding of cyber hygiene, endpoint security, multi-factor authentication (MFA), incident response, AI-driven cyber threats, cyber compliance, and digital workplace security. The program promotes a strong cybersecurity culture, helping organizations strengthen trust, protect worker information, ensure regulatory compliance, and enhance digital resilience against emerging cyber risks in the modern workplace.

Programme Curriculum

Cybersecurity Awareness for Labour Organizations Training Course

Introduction

In today’s hyperconnected digital economy, labour organizations, trade unions, worker associations, and employee representative bodies are increasingly targeted by sophisticated cyberattacks, including phishing,

ransomware, social engineering, data breaches, and identity theft. Labour organizations manage highly sensitive information such as worker records, payroll data, legal documents, collective bargaining agreements, confidential communications, and financial transactions, making them attractive targets for cybercriminals. As organizations adopt cloud computing, remote work platforms, mobile collaboration tools, and digital communication systems, the need for advanced cybersecurity awareness, data privacy protection, and cyber risk management has become critical for organizational resilience and operational continuity.

Cybersecurity Awareness for Labour Organizations Training Course equips labour organizations with practical knowledge, modern cybersecurity skills, and proactive defense strategies to identify, prevent, and respond to evolving cyber threats. Participants will gain hands-on understanding of cyber hygiene, endpoint security, multi-factor authentication (MFA), incident response, AI-driven cyber threats, cyber compliance, and digital workplace security. The program promotes a strong cybersecurity culture, helping organizations strengthen trust, protect worker information, ensure regulatory compliance, and enhance digital resilience against emerging cyber risks in the modern workplace.

Course Duration

10 Days

Course Objectives

1. Understand modern **cybersecurity threats** affecting labour organizations.
2. Identify and prevent **phishing attacks** and **social engineering scams**.
3. Strengthen **password security** and implement **multi-factor authentication (MFA)**.
4. Apply **data protection** and **privacy compliance** best practices.
5. Recognize risks associated with **remote work security** and hybrid workplaces.
6. Protect organizational systems against **ransomware** and **malware attacks**.
7. Develop effective **incident response** and **cyber crisis management** plans.
8. Improve **cloud security** and secure digital collaboration platforms.
9. Understand **AI-powered cyber threats** and emerging attack techniques.
10. Promote strong **cyber hygiene** across departments and staff levels.
11. Secure mobile devices and implement **endpoint protection** measures.
12. Build organizational resilience through **cyber risk assessment** strategies.
13. Foster a sustainable **cybersecurity awareness culture** within labour organizations.

Target Audience

1. Trade Union Leaders
2. Labour Organization Executives
3. Human Resource Professionals
4. Administrative and Finance Staff
5. IT Support Teams and System Administrators
6. Compliance and Legal Officers
7. Employee Representatives and Organizers
8. Communication and Digital Media Teams

Course Modules

Module 1: Introduction to Cybersecurity

- Fundamentals of cybersecurity

- Cyber threat landscape overview
- Importance of cybersecurity for labour organizations
- Common cyberattack methods
- Building cybersecurity awareness culture
- **Case Study:** Analysis of a labour union targeted through phishing emails leading to unauthorized access.

Module 2: Cyber Threats and Attack Vectors

- Malware, spyware, and ransomware
- Insider threats and external threats
- Social engineering tactics
- AI-powered cyberattacks
- Zero-day vulnerabilities
- **Case Study:** Ransomware attack disrupting organizational operations and payroll systems.

Module 3: Phishing and Email Security

- Identifying phishing emails
- Spear-phishing and business email compromise
- Safe email practices
- Detecting malicious attachments and links
- Email authentication basics
- **Case Study:** Employee credential theft through fake HR notification emails.

Module 4: Password and Authentication Security

- Strong password creation
- Password manager tools
- Multi-factor authentication implementation
- Credential management practices
- Preventing credential stuffing attacks

Case Study: Unauthorized access caused by weak passwords reused across platforms.

Module 5: Data Protection and Privacy

- Confidential data handling
- Personal identifiable information (PII) protection
- Data classification and retention
- Privacy regulations and compliance
- Secure file sharing practices
- **Case Study:** Data breach involving confidential employee records.

Module 6: Remote Work and Hybrid Security

- Securing remote work environments
- VPN and secure connections
- Home Wi-Fi security
- Collaboration platform risks
- Remote access policies
- **Case Study:** Security incident caused by unsecured remote desktop access.

Module 7: Mobile and Endpoint Security

- Mobile device management
- Endpoint protection tools
- Device encryption practices
- Secure use of USB devices
- Lost or stolen device response
- **Case Study:** Malware infection through unauthorized USB storage devices.

Module 8: Cloud Security Awareness

- Cloud computing fundamentals
- Cloud storage security
- Access control management
- Secure collaboration platforms
- Shared responsibility model
- **Case Study:** Exposure of confidential files due to cloud misconfiguration.

Module 9: Social Engineering Defense

- Human manipulation techniques
- Impersonation and pretexting attacks
- Vishing and smishing threats
- Psychological triggers used by attackers
- Verification and reporting procedures
- **Case Study:** Fraudulent executive impersonation requesting urgent payments.

Module 10: Ransomware Prevention and Response

- Understanding ransomware operations
- Early warning signs
- Backup and recovery strategies
- Incident containment procedures
- Business continuity planning
- **Case Study:** Organizational downtime caused by encrypted systems and ransom demands.

Module 11: Safe Internet and Social Media Use

- Secure web browsing practices
- Social media security risks
- Fake websites and online scams
- Digital footprint awareness
- Responsible online communication
- **Case Study:** Fake social media profiles targeting labour organization members.

Module 12: Incident Response and Reporting

- Cyber incident response lifecycle
- Reporting suspicious activities
- Escalation procedures
- Evidence preservation basics
- Post-incident analysis

- **Case Study:** Coordinated response to a suspected internal data leak.

Module 13: Cybersecurity Policies and Compliance

- Organizational cybersecurity policies
- Legal and regulatory compliance
- Acceptable use policies
- Security governance frameworks
- Audit and compliance readiness
- **Case Study:** Compliance gaps resulting in regulatory penalties.

Module 14: Emerging Technologies and Cyber Risks

- Artificial intelligence and cybersecurity
- Internet of Things (IoT) security
- Deepfake and synthetic media risks
- Blockchain and digital trust
- Future cyber threat trends
- **Case Study:** AI-generated voice impersonation used in fraud attempts.

Module 15: Building a Cybersecurity Culture

- Leadership roles in cybersecurity
- Employee awareness campaigns
- Cybersecurity communication strategies
- Continuous improvement approaches
- Developing long-term cyber resilience
- **Case Study:** Successful implementation of organization-wide cybersecurity awareness initiatives.

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com