SKILLSLAB
Training Provider

EVENT BROCHURE

Cybersecurity Awareness and Secure Behavior Program

Upcoming Training Event

Cairo, Egypt · 25 July 2026

Skillslab Training Provider
Skills for Tomorrow's World

info@skillslab-training.com | +966 55 965 3447 | www.skillslab-training.com

Course Description

Introduction

The **Cybersecurity Awareness and Secure Behavior Program** is a premium professional training course designed to help government entities, ministries, public sector organizations, large corporations, and executive teams strengthen their human layer of cyber defense. In today's digital operating environment, cybersecurity is no longer limited to technical controls, firewalls, or security tools; it depends heavily on the daily decisions, habits, and behaviors of employees, managers, and leaders across the organization.

This program provides a strategic and practical approach to building a security-conscious workforce capable of identifying cyber threats, reducing human error, protecting sensitive data, and responding responsibly to security incidents. It is especially valuable for organizations seeking to reduce phishing risks, improve information security compliance, protect critical systems, and create a sustainable culture of cyber resilience.

The executive-level value of this course lies in its ability to transform cybersecurity awareness from a passive compliance activity into a measurable organizational capability. Participants will gain the knowledge, confidence, and behavioral discipline required to support secure digital transformation, protect institutional reputation, and reduce operational exposure to cyberattacks.

Course Objectives

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

- Understand the role of human behavior in organizational cybersecurity risk.
- Identify common cyber threats such as phishing, social engineering, ransomware, credential theft, and business email compromise.
- Apply secure digital behavior when using email, cloud platforms, mobile devices, passwords, and corporate systems.
- Recognize warning signs of cyberattacks and suspicious online activity.
- Protect confidential, personal, financial, and government-related information from unauthorized access or disclosure.
- Follow secure practices for remote work, hybrid environments, and mobile device usage.

Course Content: 5-Day Training Outline

Day 1: Cybersecurity Awareness and the Human Risk Factor

- Understanding cybersecurity in modern government and corporate environments
- The human element in cyber risk and digital trust
- Common causes of security breaches linked to employee behavior
- Cybersecurity awareness versus secure behavior
- Key cyber threats targeting public sector and enterprise organizations
- The business impact of cyber incidents on reputation, operations, and compliance
- Building a security-first mindset across departments and leadership levels

Day 2: Phishing, Social Engineering, and Email Security

- Understanding phishing attacks, spear phishing, and executive impersonation
- How social engineering manipulates trust, urgency, authority, and emotion
- Identifying suspicious emails, links, attachments, and sender behavior
- Business email compromise and financial fraud scenarios
- Safe handling of email communications and digital requests
- Practical exercises for detecting phishing indicators
- Reporting suspicious messages through proper internal channels

Day 3: Secure Use of Passwords, Devices, Networks, and Cloud Tools

- Password security, passphrases, and credential protection
- Multi-factor authentication and access control best practices
- Secure use of laptops, smartphones, tablets, and removable media
- Risks of public networks, unsecured wireless access, and unauthorized applications
- Secure behavior in cloud collaboration platforms and shared workspaces
- Protecting accounts from credential theft and unauthorized access
- Practical workplace habits for reducing daily cyber exposure

Day 4: Data Protection, Privacy, Compliance, and Secure Communication

- Protecting sensitive, confidential, personal, and classified information

- Cybersecurity compliance expectations for government and enterprise environments
- Avoiding accidental data leakage through email, messaging, and cloud sharing

Day 5: Incident Response Behavior and Building a Cybersecurity Culture

- Recognizing early signs of cybersecurity incidents
- What to do when a security mistake happens
- Reporting incidents quickly and accurately
- Roles and responsibilities during cyber incidents
- Reducing panic, delay, and damage through proper response behavior
- Creating team-level cybersecurity habits and accountability
- Developing practical action plans for long-term secure behavior adoption

Target Audience

This course is designed for professionals and teams who need to strengthen cybersecurity awareness, improve secure workplace behavior, and reduce organizational cyber risk, including:

- Government employees and ministry staff
- Public sector professionals
- Corporate employees across operational and administrative departments
- Executive assistants and office managers
- Managers, supervisors, and team leaders
- Human resources, finance, procurement, and legal teams
- Information security awareness coordinators
- Risk, compliance, and governance professionals
- Digital transformation teams
- Employees handling sensitive, confidential, or regulated information
- Non-technical professionals who use digital systems, email, cloud tools, or enterprise applications

Course Requirements

Participants do not need an advanced technical background to attend this program. The course is designed to be practical, accessible, and relevant to both technical and non-technical professionals.

Recommended requirements include:

- Access to a laptop or smart device may be useful for selected exercises

Training Methodology

The program uses an interactive and practice-oriented training methodology designed to move participants beyond awareness into real behavioral change. The learning experience combines executive-level concepts with practical workplace application.

The methodology includes:

- Expert-led presentations using real-world cybersecurity examples
- Scenario-based learning focused on common workplace cyber risks
- Practical exercises for identifying phishing and social engineering attempts
- Group discussions on secure decision-making and organizational behavior
- Case studies from public sector and corporate cybersecurity incidents
- Guided reflection on personal and departmental cyber habits
- Action planning to improve secure behavior after the course
- Knowledge checks and applied activities to reinforce learning retention

Learning Outcomes

After completing the **Cybersecurity Awareness and Secure Behavior Program**, participants will be able to:

- Demonstrate stronger awareness of cyber threats affecting government and corporate environments.
- Make safer decisions when handling emails, links, attachments, files, systems, and sensitive information.
- Detect suspicious communication patterns and social engineering attempts more effectively.
- Apply secure password, device, network, and cloud usage practices.
- Reduce the likelihood of human-error-related cybersecurity incidents.
- Support organizational compliance with cybersecurity policies, privacy expectations, and data protection requirements.
- Respond quickly and responsibly when cyber risks or suspected incidents are identified.
- Communicate cybersecurity concerns through proper reporting channels.
- Contribute to a stronger cybersecurity culture within their department or organization.
- Align daily workplace behavior with institutional risk management and cyber resilience goals.

Instructor Profile

The instructor brings practical knowledge from real-world cybersecurity environments and provides participants with clear, actionable guidance that connects cybersecurity concepts to daily workplace decisions, public sector priorities, corporate risk exposure, and executive-level security expectations.

Strategic Value for Organizations

Organizations that invest in cybersecurity awareness and secure behavior training can significantly improve their ability to prevent, detect, and respond to cyber threats caused by human error, weak digital habits, or poor security judgment.

Contact Us

To secure your place or request further information about this event, please contact us:

Website	www.skillslab-training.com
Email	info@skillslab-training.com
WhatsApp	+966 559 653 447

Generated by Skillslab Training

info@skillslab-training.com | WhatsApp: +966 559 653 447

www.skillslab-training.com