CONCEPT

Cybersecurity Awareness Training for All Employees: Phishing, Passwords and Safe Working

19 – 23 April 2027
London - Central London four-star



Cybersecurity Awareness Training for All Employees: Phishing, Passwords and Safe Working

Ref: 1253_7474 **Date:** 19 – 23 April 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Technical depth: Practitioner · **Practical mode:** Simulation

Introduction

Most successful cyber attacks begin with an ordinary employee opening a convincing email, answering a persuasive call or reusing a weak password. Technical controls reduce the risk, but they cannot stop a person who has not learnt to recognise the warning signs or does not know how to report them. This Core Concept course, available with materials in Arabic and English, builds the everyday security habits every employee needs, from spotting phishing to handling information safely. Participants practise in realistic simulations and leave with a Personal and Team Cyber Safety Action Plan.

Course Objectives

- Recognise phishing, social engineering and impersonation attempts across email, phone, messaging and in person
- Protect work accounts with strong passphrases, multi-factor authentication and passkeys
- Handle information according to its classification when storing, sharing, printing and disposing of it
- Work securely on mobile devices, remote connections and generative AI tools
- Report suspected incidents promptly through the correct channel with the right details
- Apply a Personal and Team Cyber Safety Action Plan in daily work

Target Audience

- Administrative and office staff who handle email, documents and approvals every day
- Customer-facing staff who receive calls, messages and requests from the public
- Finance, procurement and HR staff who process payments, invoices and personal data
- Field, remote and mobile workers using laptops and phones outside the office
- Technical and operational staff without a security role who use business systems
- New joiners completing their induction into workplace security practice

Course Outline

Day 1: Why Cybersecurity Is Everyone's Job

- Confidentiality, Integrity and Availability CIA Triad in Everyday Work
- Common Attack Types: Phishing, Malware, Ransomware and Social Engineering
- The Human Factor in Attack Chains and Breach Reports
- Awareness Expectations in NIST CSF 2.0 and ISO/IEC 27001:2022 Control 6.3
- Personal Cyber Hygiene Self-Assessment Checklist

Day 2: Security Rules and Good Practice Standards

- Acceptable Use and Information Security Policy Essentials per ISO/IEC 27002
- Passphrase Practice per NIST SP 800-63B-4 and Password Managers
- Multi-Factor Authentication Methods and Passkeys
- Information Classification Labels and Clean Desk Rules
- CIS Controls v8.1 Control 14 Safeguards for the Workforce

Day 3: Safe Everyday Working

- Phishing Email Recognition Using NIST Phish Scale Cues
- Safe Web Browsing, Downloads and Removable Media Use
- Secure Remote Working, Public Wi-Fi and VPN Use
- Mobile Device Security and App Permission Settings
- Social Media Oversharing Checks and Privacy Settings

Day 4: Advanced Threats and Incident Reporting

- Business Email Compromise and Invoice Fraud Red Flags
- Vishing, Smishing and Deepfake Impersonation Calls
- Safe Use of Generative AI Tools with Work Data
- Physical Security: Tailgating, Visitor Escort and Device Theft
- Incident Recognition and Reporting Steps per ISO/IEC 27035-1

Day 5: Simulation and Personal Action Planning

- Simulated Phishing Campaign Exercise and Debrief
- Social Engineering Phone Call Simulation
- Suspicious Incident Reporting Drill
- Personal and Team Cyber Safety Action Plan Drafting
- Team Security Checklist Build and Peer Review

Skills You Will Gain

- Phishing Detection
- Social Engineering Resistance
- Account Security
- Information Handling
- Secure Remote Working
- Incident Reporting
- Safe AI Tool Use
- Security-Conscious Behaviour

Why Attend This Course

- Return to work with a Personal and Team Cyber Safety Action Plan you can apply from the first day
- Practise spotting realistic phishing emails and scam calls in a safe setting before meeting them for real
- Protect your family's accounts and devices with the same habits that protect your organisation
- Learn in Arabic or English alongside colleagues from different sectors and roles

Conclusion

Every employee is part of an organisation's defence, whether or not their job title mentions security. This course moves from why attackers target people, through the rules and good practice standards that protect accounts and information, to safe everyday working and the newer threats of invoice fraud, deepfake calls and careless use of AI tools. The final day puts participants through realistic simulations and turns the lessons into a Personal and Team Cyber Safety Action Plan that keeps good habits in place after the course.